

⑬

(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11)特許出願公表番号

特表2003-507784

(P2003-507784A)

(43)公表日 平成15年2月25日(2003.2.25)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テック・ト (参考)
G 0 6 F 12/14	3 1 0	G 0 6 F 12/14	3 1 0 K 5 B 0 1 7
1/00		12/00	5 3 7 M 5 B 0 3 5
12/00	5 3 7	G 0 6 K 19/00	Q 5 B 0 7 6
G 0 6 K 19/00		G 0 6 F 9/06	6 6 0 A 5 B 0 8 2

審查請求 未請求 予備審查請求 有 (全104頁)

(21)出願番号	特願2001-517234(P2001-517234)
(86)(22)出願日	平成12年8月11日(2000.8.11)
(85)翻訳文提出日	平成14年2月13日(2002.2.13)
(86)国際出願番号	PCT/GB00/03095
(87)国際公開番号	WO01/013198
(87)国際公開日	平成13年2月22日(2001.2.22)
(31)優先権主張番号	99306415.3
(32)優先日	平成11年8月13日(1999.8.13)
(33)優先権主張国	欧州特許庁(E P)
(31)優先権主張番号	9922669.8
(32)優先日	平成11年9月25日(1999.9.25)
(33)優先権主張国	イギリス(GB)

(71)出願人 ヒューレット・パッカード・カンパニー  
HEWLETT-PACKARD COMPANY  
アメリカ合衆国カリフォルニア州パロアル  
ト ハノーバー・ストリート 3000

(72)発明者 ビアソン, シアニ, ライン  
イギリス国ブリストル・ビーエス9・3ビ  
ーゼット, ウェストバーリー・オン・トリ  
ム, サンディリーズ・35

(74)代理人 弁理士 古谷 翳 (外3名)

**最終頁に続く**

(54)【発明の名称】 記憶されたデータの使用に対する強制的な制限

(57) 【要約】

コンピュータシステムは、データ上の操作を制限するように適合される。コンピュータシステムは、プラットフォームのユーザがデータに対してリクエストされた操作を行なうことを許諾されているかどうかをチェックするため、及びデータの使用を可能にするためのセキュリティレベルを有するコンピュータプラットフォームと、ユーザのアイデンティティを含む携帯型の信用されるモジュールと、その信用されるモジュールが予想された態様で動作し、無許可の外部の修正に抵抗するように適合されたコンポーネントであることと、及びデータに関連してユーザのライセンス許諾を指定するアクセスプロファイルとを含む。有利な点は、コンピュータプラットフォームが、プラットフォームの信用されるモジュールを含み、このモジュールは、携帯型の信用されるモジュールとの相互認証に従事し、セキュリティレベルを含む。セキュリティレベルは、リクエストされた操作が携帯型の信用されるモジュールに含まれるユーザのアイデンティティに対して許諾されているかどうかを判定するために、アクセスプロファイルをチェックするように適合される。セキュリティレベルは、ライセンスが必要であって存在しない場合、リクエストされた操作を止める。

[illegible]

**【特許請求の範囲】**

【請求項1】 データに対する操作を制限するように適合されたコンピュータシステムであって、

プラットフォームのユーザが、データに対してリクエストされた操作を行なうために許諾されているかどうかをチェックし、データの使用を可能にするためのセキュアオペレータを有するコンピュータプラットフォームと、

ユーザのアイデンティティを含む携帯型の信用されるモジュールと、その信用されるモジュールが、予想された態様で動作し、無許可の外部の修正に抵抗するように適合されたコンポーネントであることと、及び

データに関してユーザのライセンス許諾を指定するアクセスプロファイルとを含み、

前記セキュアオペレータが、前記携帯型の信用されるモジュールに含まれたユーザのアイデンティティに対してリクエストされた操作が許諾されているかどうかを判定し、ライセンスが必要であって存在しない場合、リクエストされた操作を止めるために、アクセスプロファイルをチェックするように適合されている、コンピュータシステム。

【請求項2】 前記コンピュータプラットフォームが、プラットフォームの信用されるモジュールをさらに含み、そのプラットフォームの信用されるモジュール及び前記携帯型の信用されるモジュールが、相互に認証するように適合されている、請求項1に記載のコンピュータシステム。

【請求項3】 前記セキュアオペレータのいくつか又はすべての機能性が、前記プラットフォームの信用されるモジュール内にある、請求項2に記載のコンピュータシステム。

【請求項4】 前記アクセスプロファイルが、前記コンピュータプラットフォーム内にある、請求項1～3のいずれかに記載のコンピュータシステム。

【請求項5】 いくつか又はすべてのデータが、前記コンピュータプラットフォーム内にあり、前記コンピュータプラットフォームは、前記コンピュータプラットフォームのプロセッサがデータに対する操作を実行する前に、データの完全性をチェックするためのデータプロテクタをさらに含む、請求項1～4のいずれかに記

載のコンピュータシステム。

【請求項6】いくつか又はすべてのデータが、前記携帯型の信用されるモジュール内、又は前記携帯型の信用されるモジュールを含む装置内にあり、前記携帯型の信用されるモジュール又は前記携帯型の信用されるモジュールを含む装置は、前記コンピュータプラットフォームのプロセッサがデータに対する操作を実行する前に、データの完全性をチェックするためのデータプロテクタをさらに含む、請求項1～4のいずれかに記載のコンピュータシステム。

【請求項7】前記データプロテクタが、関連する信用されるモジュール内にある、請求項5又は請求項6に記載のコンピュータシステム。

【請求項8】前記データプロテクタが、データのインストールをチェックし、保護されたデータの要約及び／又は関連する信用されるコンポーネントへの任意の関連するアクセスプロファイルをロードするように適合されている、請求項5～7のいずれかに記載のコンピュータシステム。

【請求項9】前記信用されるプラットフォームが、前記セキュアオペレータ及び存在するならば前記データプロテクタを含む操作保護コードの完全性をブートにおいてチェックするように適合されている、請求項1～8のいずれかに記載のコンピュータシステム。

【請求項10】前記コンピュータプラットフォームが、第1のハッシュを生成するために前記操作保護コードを読取ってハッシュし、第2のハッシュを生成するために前記プラットフォームの信用されるモジュールに記憶された第三者の公開鍵証明を使用してセキュア操作保護コードハッシュの記憶されたサイン済みバージョンを読取って暗号解読し、及び前記第1のハッシュと前記第2のハッシュとを比較することによって、完全性チェックを行なうように適合されている、請求項2に従属する場合の請求項9に記載のコンピュータシステム。

【請求項11】前記携帯型の信用されるモジュールが、取り外し可能な信用されるモジュールに関連するデータにアクセスする権利を指定するユーザアクセスライセンスを含み、それにより前記アクセスプロファイルによって止められるまで、前記セキュアオペレータが、携帯型の信用されるモジュールに含まれるユーザのアイデンティティに対してリクエストされた操作が許諾されているかどうか

かを判定するために、ユーザアクセスライセンスをチェックするように適合されている、請求項1～10のいずれかに記載のコンピュータシステム。

【請求項12】前記コンピュータプラットフォームが、前記プラットフォームの信用されるモジュールとコンピュータプラットフォームのオペレーティングシステムとの間にセキュア通信経路を含む、請求項2に従属する場合の前記請求項のいずれかに記載のコンピュータシステム。

【請求項13】コンピュータプラットフォームは、

前記オペレーティングシステムが、ターゲットデータの名称および意図した操作を送信することによって、データに作用する前にセキュアオペレータからのポリシーチェックをリクエストし、

前記セキュアオペレータが、データを操作させてもよいかどうかを判定するために前記アクセスプロファイルにおけるターゲットデータに関連する制限をチェックし、及び

前記セキュアオペレータが、制限を有する申し込まれた使用をチェックし、オペレーティングシステムに応答するように適合されている、請求項1～13のいずれかに記載のコンピュータシステム。

【請求項14】データに対する操作の許可のために前記オペレーティングシステムがリクエストする際、前記セキュアオペレータが、前記プラットフォームの信用されるモジュールの秘密鍵によってサインされたアクセスプロファイルにメッセージを送信し、前記アクセスプロファイルが、前記プラットフォームの信用されるモジュールの公開鍵にアクセスし、その公開鍵によってサインされたメッセージを確認して認証することができ、それにより満たされた場合、前記アクセスプロファイルが、前記セキュアオペレータにアクセスプロファイルデータを送信し、その結果、前記セキュアオペレータが、前記アクセスプロファイルデータをテストし、適切な場合、前記オペレーティングシステムにリクエストされた操作を実行することをリクエストする、請求項3に従属する場合の請求項13に記載のコンピュータシステム。

【請求項15】前記関連した信用されるコンポーネントが、データ及び関連するアクセスプロファイル上で一方向機能のセキュア結果を含み、その一方向機

能の計算がセキュア結果と異なった結果を提供した場合、前記データプロテクタが、操作の実行を止める、請求項2及び請求項5～7のいずれかに従属する請求項13又は請求項14に記載のコンピュータシステム。

【請求項16】前記プラットフォームの信用されるコンポーネントが、データにおける特定の操作を実行するために、前記オペレーティングシステムに対するリクエストをログ記録するように適合されている、請求項2に従属する場合の前記請求項のいずれかに記載のコンピュータシステム。

【請求項17】前記携帯型の信用されるコンポーネントが、データに対する特定の操作を実行するために、前記オペレーティングシステムに対するリクエストをログ記録するように適合されている、請求項6に記載のコンピュータシステム。

【請求項18】データに対する操作を制限するように適合されたコンピュータシステムであって、

データに関してユーザのライセンス許諾を指定し、データの使用を可能にするためのアクセスプロファイルを有するコンピュータプラットフォームと、

ユーザのアイデンティティを含む携帯型の信用されるモジュールと、信用されるモジュールが、予想された態様で動作し、無許可の外部の修正に抵抗するように適合されたコンポーネントであることとを含み、

前記アクセスプロファイルが、前記携帯型の信用されるモジュールに含まれたユーザアイデンティティに対してリクエストされた操作が許諾されているかどうかを判定し、ライセンスが必要であって存在しない場合、リクエストされた操作を止めるように適合されている、コンピュータシステム。

【請求項19】前記コンピュータプラットフォームのオペレーティングシステムが、データに対する所定の操作を実行する前に、前記アクセスプロファイルからのポリシーチェックをリクエストするように適合され、その結果、前記アクセスプロファイルが、データを操作してもよいかどうかを判定するために、データに加える制限をチェックし、それにしたがって前記オペレーティングシステムに応答する、請求項18に記載のコンピュータシステム。

【請求項20】プラットフォームのユーザが、データに対してリクエストされ

た操作を行なうために許諾されているかどうかをチェックし、データの使用を可能にするためのセキュアオペレータを有するコンピュータプラットフォームと、

ユーザのアイデンティティを含む携帯型の信用されるモジュールと、信用されるモジュールが、予想された態様で動作し、無許可の外部の修正に抵抗するように適合されたコンポーネントであることと、及び

データに関してユーザのライセンス許諾を指定するアクセスプロファイルとを含むシステムにおいて、データの操作を制限する方法であって、

その方法が、前記セキュアオペレータにターゲットデータの名称および意図した操作を送信することによって、データに作用する前に前記セキュアオペレータに前記コンピュータプラットフォームのオペレーティングシステムによるポリシーチェックのためのリクエストを含み、

前記セキュアオペレータが、データを操作してもよいかどうかを判定するために前記アクセスプロファイルのターゲットデータに関連する制限をチェックし、及び

前記セキュアオペレータが、制限を有する申し込まれた使用をチェックし、前記オペレーティングシステムに応答する、方法。

【請求項21】前記コンピュータプラットフォームが、プラットフォームの信用されるモジュールをさらに含み、前記セキュアオペレータのいくつか又はすべての機能が、前記プラットフォームの信用されるモジュール内にあり、それによりデータに対する操作の許諾のために前記オペレーティングシステムがリクエストする際、前記セキュアオペレータが、前記プラットフォームの信用されるモジュールの秘密鍵によってサインされたアクセスプロファイルにメッセージを送信し、前記アクセスプロファイルが、前記プラットフォームの信用されるモジュールの公開鍵にアクセスし、かつその公開鍵によってサインされたメッセージを確認して認証することができ、それにより、満たされた場合、前記アクセスプロファイルが、前記セキュアオペレータにアクセスプロファイルデータを送信し、その結果、前記セキュアオペレータが、前記アクセスプロファイルデータをテストし、適切な場合、前記オペレーティングシステムにリクエストされた操作を実行することをリクエストする、請求項20に記載の方法。

【請求項22】前記コンピュータプラットフォームが、データに対する操作をコンピュータプラットフォームのプロセッサが実行する前に、データの完全性をチェックするためのデータプロテクタをさらに含み、前記プラットフォームの信用されるコンポーネントが、データ及び関連するアクセスプロファイルに対する一方向機能のセキュア結果を含み、その一方向機能の計算がセキュア結果と異なった結果を提供した場合、前記データプロテクタが、操作の実行を止める、請求項21に記載の方法。

【請求項23】データの実行の前に、前記データプロテクタが、前記コンピュータプラットフォーム内に記憶されたデータの複数のコピーがないことをチェックし、複数のコピーがあった場合、データの実行を止める、請求項21に記載の方法。

【請求項24】前記コンピュータプラットフォームが、前記プラットフォームの信用されるコンポーネントと前記オペレーティングシステムとの間にセキュア通信経路を含み、それによりデータを使用するために前記セキュアオペレータから前記オペレーティングシステムへのリクエストが、前記セキュア通信経路に提供される、請求項21に記載の方法。

【請求項25】前記プラットフォームの信用されるモジュールが、データに対する特定の操作を実行するために、前記オペレーティングシステムへの任意のリクエストをログ記録するように適合されている、請求項21に記載の方法。

【請求項26】制限された使用に関してコンピュータプラットフォームにデータをインストールする方法であって、そのコンピュータプラットフォームが、

プラットフォームのユーザがデータに対してリクエストされた操作を行なうために許諾されているかどうかをチェックし、データの使用を可能にするためのセキュアオペレータを有するコンピュータプラットフォームと、

プラットフォームの信用されるモジュールと、信用されるモジュールが、予想された態様で動作し、無許可の外部の修正に抵抗するように適合されたコンポーネントであることと、及び

データに対する操作を前記コンピュータプラットフォームのプロセッサが実行する前に、データの完全性をチェックするためのデータプロテクタとを含み、

前記方法が、データ及び関連するアクセスプロファイルのインストールの前にデータの信頼性の証明を含み、前記プラットフォームの信用されるモジュールへ保護されたデータの要約及び関連するアクセスプロファイルをロードし、それによりその要約が、データを実行する前に、前記データプロテクタ及び／又はセキュアオペレータによって使用される、方法。

【請求項27】プラットフォームのユーザがデータに対してリクエストされた操作を行なうために許諾されているかどうかをチェックし、データの使用を可能にするためのセキュアオペレータと、及びデータに関するユーザのライセンス許諾を指定するアクセスプロファイルとを有し、コンピュータプラットフォームとの通信において携帯型の信用されるモジュールに含まれるユーザのアイデンティティに対してリクエストされた操作が許諾されているかどうかを判定するために、セキュアオペレータが、アクセスプロファイルをチェックするように適合されており、信用されるモジュールが、予想された態様で動作し、無許可の外部の修正に抵抗するように適合されたコンポーネントであり、ライセンスが必要とされて存在しない場合、リクエストされた操作を止めるように適合されている、コンピュータプラットフォーム。

【請求項28】プラットフォームの信用されるモジュールをさらに含み、そのプラットフォームの信用されるモジュール及び前記携帯型の信用されるモジュールが、相互に認証するように適合されている、請求項27に記載のコンピュータプラットフォーム。

【請求項29】前記セキュアオペレータのいくつか又はすべての機能性が、前記プラットフォームの信用されるモジュール内にある、請求項28に記載のコンピュータプラットフォーム。

【請求項30】前記アクセスプロファイルが、前記プラットフォームの信用されるモジュール内にある、請求項27～29のいずれかに記載のコンピュータプラットフォーム。

【請求項31】いくつか又はすべてのデータが、前記コンピュータプラットフォーム内にあり、前記コンピュータプラットフォームは、コンピュータプラットフォームのプロセッサがデータに対する操作を実行する前に、データの完全性をチェ



ックするためのデータプロテクタをさらに含む、請求項27～30のいずれかに記載のコンピュータプラットフォーム。

【請求項32】前記データプロテクタが、前記プラットフォームの信用されるモジュール内にある、請求項31に記載のコンピュータプラットフォーム。

【請求項33】前記データプロテクタが、データのインストールをチェックし、保護されたデータの要約及び／又は前記プラットフォームの信用されるコンポーネントへ任意の関連するアクセスプロファイルを読み込むように適合されている、請求項31又は請求項32に記載のコンピュータプラットフォーム。

【請求項34】前記コンピュータプラットフォームが、前記セキュアオペレータ及び存在するならば前記データプロテクタを含む操作保護コードの完全性をブートにおいてチェックするように適合されている、請求項27～33のいずれかに記載のコンピュータプラットフォーム。

【請求項35】前記プラットフォームの信用されるモジュールと前記コンピュータプラットフォームのオペレーティングシステムとの間のセキュア通信経路をさらに含む、請求項28に記載のコンピュータプラットフォーム。

【請求項36】前記オペレーティングシステムが、データの名称および意図した操作を送信することによって、データに作用する前に前記セキュアオペレータからポリシーチェックをリクエストし、

前記セキュアオペレータが、データを操作してもよいかどうかを判定するために前記アクセスプロファイルにおけるターゲットデータに関連する制限をチェックし、及び

前記セキュアオペレータが、制限を有する申し込まれた使用をチェックし、前記オペレーティングシステムに回答するように適合された、請求項27～35のいずれかに記載のコンピュータプラットフォーム。

【請求項37】データに対する操作の許可のために前記オペレーティングシステムがリクエストする際、前記セキュアオペレータが、前記プラットフォームの信用されるモジュールの秘密鍵によってサインされたアクセスプロファイルにメッセージを送信し、前記アクセスプロファイルが、前記プラットフォームの信用されるモジュールの公開鍵にアクセスし、その公開鍵によってサインされたメッセ

ージを確認して認証することができ、それにより満たされた場合、前記アクセスプロファイルが、前記セキュアオペレータにアクセスプロファイルデータを送信し、その結果、前記セキュアオペレータが、前記アクセスプロファイルデータをテストし、適切な場合、前記オペレーティングシステムにリクエストされた操作を実行することをリクエストする、請求項28に従属する場合の請求項36に記載のコンピュータプラットフォーム。

【請求項38】前記プラットフォームの信用されるコンポーネントが、データ及び関連するアクセスプロファイル上で一方向機能のセキュア結果を含み、その一方向機能の計算がセキュア結果と異なった結果を提供した場合、前記データプロテクタが、操作の実行を止める、請求項28に従属する請求項31に記載のコンピュータプラットフォーム。

【請求項39】ユーザのアイデンティティを含む携帯型の信用されるモジュールであって、信用されるモジュールが、予想された態様で動作し、無許可の外部の修正に抵抗するように適合されたコンポーネントであり、前記携帯型の信用されるモジュールが、移動可能な信用されるモジュールに関連するデータにアクセス権利を指定するユーザアクセスライセンスを含む、携帯型の信用されるモジュール。

【請求項40】スマートカード内に配置される、請求項39に記載の携帯型の信用されるモジュール。

【請求項41】データに関するユーザのライセンス許諾を指定し、データの使用を可能にするためのアクセスプロファイルを有するコンピュータプラットフォームと、

ユーザのアイデンティティを含む携帯型の信用されるモジュールと、信用されるモジュールが、予想された態様で動作し、無許可の外部の修正に抵抗するように適合されたコンポーネントであることとからなるシステムにおいて、データの操作を制限する方法であって、

その方法が、前記アクセスプロファイルにターゲットデータの名称および意図した操作を送信することによって、データに作用する前に前記アクセスプロファイルに前記コンピュータプラットフォームのオペレーティングシステムによるポリ

シーチェックのためのリクエストを含み、

前記アクセスプロファイルが、データを操作してもよいかどうかを判定するためにターゲットデータに関連する制限をチェックし、前記オペレーティングシステムに応答する、方法。

【請求項42】前記コンピュータプラットフォームが、プラットフォームの信用されるモジュールを含み、前記アクセスプロファイルのいくつか又はすべての機能性が、前記プラットフォームの信用されるモジュール内にある、請求項41に記載の方法。

## 【発明の詳細な説明】

## 【0001】

## 【発明が属する技術分野】

本発明は、コンピュータプラットフォーム、及びその動作方法に関し、より具体的には、コンピュータプラットフォームにおける、特に多数のモバイルユーザに使用可能なコンピュータプラットフォームにおけるデータの使用の制御及び／又は計測 (metering) に関する。

## 【0002】

本明細書において、「データ」とは、画像、ソフトウェア及びストリーミング媒体のように、デジタル的にフォーマット化することができるあらゆるものを意味する。

## 【0003】

## 【従来の技術】

将来、コンピュータシステムは、オペレーティングシステム及び搭載されたソフトウェアにウィルス又は他の無許可の修正が行なわれないことを保証するために、別のコードにおける完全性のチェックと共に、それ以上のセキュアブーティングを達成することができるであろう。さらに、新しい世代の改竄防止装置は、すでに現われており又はすぐに市場に現われようとしており、かつ外部又は携帯型のコンポーネント (スマートカードのような) 及び内部のコンポーネント (組み込み型プロセッサ、半組み込み型プロセッサ又はセキュリティー機能性を有するコプロセッサ、すなわちマザーボード、USB及びISAによる実施を含む) 両方を含んでいる。これらの改竄防止コンポーネントは、システムのハードウェアが不正変更を受けたことをチェックし、現在使用できるもの (例えば、マシンのイーサネット (R) 名称) よりも信頼できるマシンのアイデンティティ (identity : 識別性) の形式を提供するために使用されるであろう。2000年2月15日に出願され、「Trusted Computing Platform」と題する本出願人の継続中の国際特許出願第PCT/GB00/00528号は、信頼できる測定及び信頼できる完全性のメトリックスの報告によって、コンピュータプラットフォームの完全性の証明を可能にするように適合されているシステムを記載し、その全内容は

これをもって参照により本明細書に組み込まれる。これは、ローカルユーザ又はリモートエンティティによって、プラットフォームの完全性の証明を可能にする。

#### 【0004】

このような改竄防止コンポーネント及びセキュアブーティングの可能性の存在は、それ自体によってコンピューティングプラットフォームの使用に関するすべてのセキュリティの問題を取り除くわけではない。特に著作権侵害の阻止、及びソフトウェア開発者及びエンドユーザに受け入れることができるようなソフトウェア使用の使用許諾 (licencing) 及び計測は、いぜんとして主要な問題を提供している。

#### 【0005】

ソフトウェア使用許諾は、ハッキングと著作権侵害を受けやすく、現在の使用されるすべてのソフトウェア使用許諾方法は、これらの関連する問題を有する。使用許諾のソフトウェアによる実施（「ライセンスマネージメントシステム」のような）は、融通性を有するが、とりわけ安全又は敏速ではない。特に、これらは、セキュリティの不足（例えば一般的な「ハッキング」を受ける）、及びソフトウェアの真の置き換えの困難に悩まされている。逆に、ハードウェアによる実施（「dongle」）は、ソフトウェアによる実施に比べて高速であり、一般に安全であるが、融通性がない。これらは、ソフトウェアの特定の部分に対してだけ適応されており、エンドユーザに対しては不便である。

#### 【0006】

ライセンス保護の分野における一般的な技術は、使用許諾及び他の保護処置に関する情報をコード化するためにソフトウェアラッパを使用することである。データラッパ又は暗号コンテナは、一般にソフトウェアだけに使用され、データ保護のハイブリッド法は、完全性チェックがラッパ内に含まれている場合でさえ、変更及び除去に対して傷付きやすいので、現在、保護のきわめて安全な方法というわけではない。特に、データラッパは、ハッカに対する第1のターゲットである。なぜならこれは、データを実行することができる方法を管理するデータの開発者によって定義されるプロファイル、又は変更してはいけない他のデリケートな情報を含むことができるからである。認証、暗号化及び完全性のチェックを用

いて、顧客のプラットフォームにダウンロードされ、記憶されている途中で修正されることに対してラッパを保護することができる。しかしながら、データ及び関連するラッパが、顧客のプラットフォーム内に一度記憶されると（例えば、ハードディスク上に）、悪意の存在によって又は事故によって修正され又は消去される可能性があるという重大な危険性が存在する。一度修正されると、データは、ある意味で当初の修正されていないラッパにおいて定義されたプロファイルの範囲の外側にある顧客のプラットフォームで使用されることがある。

#### 【0007】

このような困難に対処する1つのシステムは、「Persistent Access Control to Prevent Piracy of Digital Information」、Paul B. Schneck著、Proceeding of the IEEE、第87巻、第7号、1999年7月、第1239-1250頁に提案されており、これは、データにアクセスする前に、使用許諾情報をチェックするためにアクセス制御ソフトウェアを使用する。しかしながら、そのシステムは、一般的なライセンス（許可）がすべてのユーザに対して使用可能である場合だけを考慮している。アクセス制御機構は、この問題に対する完全な解決策を提供することができない。なぜなら、これらは、バイパスされることができ、さらにこれらは、データの開発者ではなくユーザの管理者によって指定される制御的を絞っているからである。種々のソフトウェア許諾を有するユーザによってプラットフォームが共有される多くの状況が存在する。既存のシステムは、おそらくますます重要になるこの問題に満足に対処していない。

#### 【0008】

##### 【本発明の概要】

したがって、本発明は、データに対する操作を制限するように適合されたコンピュータシステムを提供し、このコンピュータシステムは、プラットフォームのユーザがデータに対してリクエストされた操作を行なうために許諾されているかどうかをチェックし、データの使用を可能にするためのセキュアオペレータを有するコンピュータプラットフォームと、ユーザのアイデンティティを含む携帯型の信用されるモジュールと、その信用されるモジュールが、予想された態様で動作し、無許可の外部の修正に抵抗するように適合されたコンポーネントであることと

、及びデータに関してユーザのライセンス許諾を指定するアクセスプロファイルとを含み、セキュアオペレータが、携帯型の信用されるモジュールに含まれたユーザアイデンティティに対してリクエストされた操作が許諾されているかどうかを判定し、ライセンスが必要であって存在しない場合、リクエストされた操作を止めるために、アクセスプロファイルをチェックするように適合されている。好適には、コンピュータプラットフォームは、プラットフォームの信用されるモジュールをさらに含み、そのプラットフォームの信用されるモジュール及び携帯型の信用されるモジュールが、相互に認証するように適合されている。

#### 【0009】

本発明は、コピー、変更又は実行のように、データにおいて行なうことができる操作を防止し、制限するために使用されるソフトウェアラップ又は他のタイプのデータ許可に適用可能である。本発明の特に好適な形態は、2つの信用されるモジュール(TC)を使用し、これらのモジュールの第1のものは、典型的にスマートカードに保持される携帯型のTCであり、第2のものは、コンピュータプラットフォームの一部である。これらは、データが開発者によって指定された方法において携帯型のTCの所有者によってのみ使用できることを確実にするために、ソフトウェアに関連して使用され、好適にはTC内において動作する。

#### 【0010】

システムの好適な実施形態において、いくつか又はすべてのデータは、携帯型の信用されるモジュール内、又は携帯型の信用されるモジュールを含む装置内にあり、携帯型の信用されるモジュール又は携帯型の信用されるモジュールを含む装置は、コンピュータプラットフォームのプロセッサがデータに対する操作を実施する前に、データの完全性をチェックするためのデータプロテクタをさらに含む。この構成は、データが(アクセスプロファイル又はラップと共に)、信用される顧客のプラットフォームに記憶された後に、関連するアクセスプロファイル又は他のタイプのラップが変化されておらず又は消去されていないことのチェックを提供する利点を有する。

#### 【0011】

本発明は、ユーザのアイデンティティ(スマートカードのように移動可能なT

Cから導出される) にしたがってアクセスチェックが行なわれる顧客のシステムを使用する点において、シュネッケのシステムと相違するが、チェックそれ自体は、顧客のPC又は他の顧客のプラットフォームに搭載されたアクセス制御ソフトウェアを使用して行なわれる。さらに次のことが可能である。すなわち、(a) ライセンスは、所定のタイプのアクセス制御のために必要なPC TCの代わりに又はそれと同様に、それぞれのエンドユーザに関連することができ、(b) データが暗号化されていることは必須のことではなく(好適ではあるが)、(c) ライセンスの修正を防ぐために(アクセスプロファイル参照)、要約は、ロードの際にTCに記憶され、データアクセスの前に調べられ、(d) アクセス制御コードは、BIS (BOOT Integrity Service) において保護され、好適にはTC内において動作し、さもないとコードとコンピュータプラットフォームの他の部分にアクセス不可能なTCとの間に専用の通信経路があり、(e) ログ記録がTC内において行なわれ、及び(f) ライセンスがさらに事前対応の役割を有することができる。

#### 【0012】

この特定の発明の動機付けは、データ使用法のさらに複雑なモデルがさらに大きな融通性を要求し、この融通性は、顧客のプラットフォームにおける複数のTCを使用することによってのみ実質的にもたらされ得る。特に事務所の環境におけるホットデスクング(hot-desking)又は空港のような公共の場所における共有端末からのアクセス情報又はサービスインは、共有の顧客の機械におけるTCを有することによって、及びこのユーザを識別する少なくとも1つの携帯型TCによって発行されたそれぞれのユーザによってモデル化することができる。本発明の適切な実施形態の使用によって、データに対して行なわれる操作の妥当性をチェックするソフトウェアと共にデータに関連したユーザのライセンスを介して、記憶されたデータの使用に対する強制的な制限によって、モバイルユーザが信用されるコンピュータプラットフォームにおいて汎用のデータアクセスを行なうことを可能にする。ユーザのライセンスは、スマートカードのような携帯型の信用される装置に記憶することができ、又はそれにより発行されることができ、データと共にダウンロードされることができ、又はデータから独立して送信することが



できる。インストール以後、データが修正されていないことを保証するために、データにおける完全性のチェックを行なうためのオプションが存在する。従って、コピーのようなデータにおける無許可の操作は、データの修正又は同じプラットフォームにおけるその関連するライセンスと共に防止することができる一方で、ユーザは、データアクセスのホットデスクキングモデルから利益を得ることができる。

#### 【0013】

本発明の実施形態は、個々のユーザに、そのユーザだけが利益を得ることになるデータアクセスに対して支払いを行なうことを可能にする。ユーザは、持ち歩くことができる改竄防止の携帯型装置にこのようなライセンスを獲得することができ、例えその場所がどこであっても、任意の信用されるプラットフォームにおいて使用することができる。代案として、信用されるプラットフォームに保持された個々のライセンスは、携帯型のモジュールのセキュアIDを参照するためにカスタマイズすることができる。データそれ自体が携帯型の装置において獲得された場合、データを顧客の機械にインストールする必要はない。必要に応じて、データは、リクエストされた際に、すでにインストールされていないならば、ダウンロードすることができる。

#### 【0014】

1つの態様において、本発明は、プラットフォームのユーザがデータに対してリクエストされた操作を行なうために許諾されているかどうかをチェックし、データの使用を可能にするためのセキュアオペレータ、及びデータに関するユーザのライセンス許諾を指定するアクセスプロファイルを有するコンピュータプラットフォームを提供し、コンピュータプラットフォームとの通信において携帯型の信用されるモジュールに含まれるユーザのアイデンティティに対してリクエストされた操作が許諾されているかどうかを判定するために、セキュアオペレータが、アクセスプロファイルをチェックするように適合されており、信用されるモジュールが、予想された態様で動作し、無許可の外部の修正に抵抗するように適合されたコンポーネントであり、ライセンスが必要とされていて存在しない場合、リクエストされた操作を止めるように適合されている。

## 【0015】

別の態様において、本発明は、ユーザのアイデンティティを含む携帯型の信用されるモジュールを提供し、信用されるモジュールが、予想された態様で動作し、無許可の外部の修正に抵抗するように適合されたコンポーネントであり、携帯型の信用されるモジュールが、移動可能な信用されるモジュールに関するデータに対するアクセス権利を指定するユーザアクセス許可を含む。

## 【0016】

本発明の特に好適な実施形態は、開発者によって指定された記憶済みデータの、それぞれの個々のエンドユーザによる使用に関する制限が遵守されなければならないこと、種々のエンドユーザが異なったアクセスプロファイルを有することができること、さらにデータ又は関連するラップ又はライセンスがプラットフォームへの初期のダウンロードから修正されていた場合、データがプラットフォームにおいて使用できないことを保証する、コンピュータプラットフォーム（これはおそらく幾つかのユーザによって共有される）の信用されるモジュール（TC）を、好適にはTC内において動作するソフトウェアに関連して使用する。ホストCPUは、TCにターゲットデータの名称および意図した操作を送信することによって、データに作用する前にポリシーチェックをリクエストする。TCは、ログインされた（携帯型のTCのIDを介して）ユーザのID、及びターゲットデータに関連するこの現在のエンドユーザに対応する制限をチェックする。これらの制限は、だれがデータにアクセスしてもよいか、データを使用できる回数、行なってはいけない操作等に関するものであり、または制限は、意図的「NULL（ヌル）」としてロードされていてもよい。TCは、制限と共に提案された使用をチェックする。適切な許諾が見つからなかった場合、TCは、携帯型のTC（有利にはスマートカード）におけるライセンスについて、及びこの範囲内のデータ使用に対する有効な許諾についてチェックする。次いで、TCは、適宜、アクセス許諾を備えて、又は備えることなしにCPUに応答する。このようにCPUは、TCから適切な許諾を取得することなく、コピー、編集、セクションの追加、セクションの置き換え、実行、消去、プリント、オープン、スキャン、名称変更、位置の移動、送信又は読出しのようなターゲットデータに対する所定の操作を行なう

ことができない。好適には、ターゲットデータ及び制限の完全性は、これらがプラットフォームにおいて非合法的に又は偶発的に修正されていないことを保証するために、操作を実施する前にチェックされる。その代わりにチェックは、携帯型のTC自体で実行してもよい。

#### 【0017】

システムの重要なコンポーネントは、アプリケーションソフトウェア又はデータのそれぞれの部分に関連したアクセスプロファイルであり、これは、保護すべきデータを指定し、その特定のソフトウェア又はデータにおいて実行されることを開発者が望んだ操作のタイプを指定する。必要に応じて、アクセスプロファイルは、特定のTC ID、又はTC又は現在サインされているスマートカードについてチェックすべき秘密（secret）のような所定の操作を実施することについてチェックすべき他の任意の特定の情報を指定する。別の可能性は、TC又はスマートカード（適切にセグメント化されている）内において、好適にはデータと共に動作するアクセスプロファイルに関するものである。アクセスプロファイルは、データに関連するライセンスの形態、又は暗号のコンテナと考えることができる。

#### 【0018】

別の態様において、本発明は、データに対する操作を制限するように適合されたコンピュータシステムを提供し、このコンピュータシステムは、データに関してユーザのライセンス許諾を指定し、データの使用を可能にするためのアクセスプロファイルを有するコンピュータプラットフォームと、ユーザのアイデンティティを含む携帯型の信用されるモジュールと、その信用されるモジュールが、予想された態様で動作し、無許可の外部の修正に抵抗するように適合されたコンポーネントであることとを含み、アクセスプロファイルが、携帯型の信用されるモジュールに含まれたユーザアイデンティティに対してリクエストされた操作が許諾されているかどうかを判定し、ライセンスが必要であって存在しない場合、リクエストされた操作を止めるように適合されている。

#### 【0019】

さらに別の態様において、本発明は、システムにおけるデータに対する操作を

制限する方法を提供し、このシステムが、データに関するユーザのライセンス許諾を指定し、データの使用を可能にするためのアクセスプロファイルを有するコンピュータプラットフォームと、ユーザのアイデンティティを含む携帯型の信用されるモジュールと、その信用されるモジュールが、予想された態様で動作し、無許可の外部の修正に抵抗するように適合されたコンポーネントであることとを含み、方法が、アクセスプロファイルにターゲットデータの名称および意図した操作を送信することによって、データに作用する前にアクセスプロファイルにコンピュータプラットフォームのオペレーティングシステムによるポリシーチェックのためのリクエストを含み、アクセスプロファイルが、データを操作してもよいかどうかを判定するためにターゲットデータに関連する制限をチェックし、オペレーティングシステムに応答する。

#### 【0020】

本発明のこれらの態様において、アクセスプロファイルは、さらに事前対応な役割を引き受ける。アクセスプロファイルは、セキュアオペレータというよりはむしろ制限されたデータを実行するオペレーティングシステムの能力を制御する役割を引き受ける。

#### 【0021】

さらに別の態様において、本発明は、システムにおけるデータに対する操作を制限する方法を提供し、このシステムが、プラットフォームのユーザが、データに対するリクエストされた操作を行なうために許諾されているかどうかをチェックし、データの使用を可能にするためのセキュアオペレータを有するコンピュータプラットフォームと、ユーザのアイデンティティを含む携帯型の信用されるモジュールと、その信用されるモジュールが、予想された態様で動作し、無許可の外部の修正に抵抗するように適合されたコンポーネントであることと、及びデータに関してユーザのライセンス許諾を指定するアクセスプロファイルとを含み、方法が、セキュアオペレータにターゲットデータの名称および意図した操作を送信することによって、データに作用する前にセキュアオペレータにコンピュータプラットフォームのオペレーティングシステムによるポリシーチェックのためのリクエストを含み、セキュアオペレータが、データを操作してもよいかどうかを判定す

るためにアクセスプロファイルにおけるターゲットデータに関連する制限をチェックし、セキュアオペレータが、制限を有する申し込まれた使用をチェックし、オペレーティングシステムに応答する。

#### 【0022】

本発明による操作の好適な方法において、サインオンの際、移動可能なモジュール及びPC TCは、相互に認証し、TCは、移動可能なモジュールの識別子を記憶する。保護されたデータが使用できる前に、セキュアオペレータ又はデータに関連するアクセスプロファイル（使用される特定のモジュールに応じて）は、OSに特定の操作を実行するための許諾を与える必要がある。データに関する制限のチェックの際、セキュアオペレータ又はアクセスプロファイルは、ユーザのアイデンティティに関する制限チェックを実行するように動作することができる。ライセンスがスマートカード内に記憶されている場合、セキュアオペレータは、今後、調べることができ、さもなければライセンスの詳細を見出すごとにスマートカードを調べることができるTC PCに保持されたライセンスを記憶装置内に取り込む必要がある。このユーザライセンスは、データアクセスの結果として更新することができ、例えば、操作許諾がユーザの固定番号に対するものであることによって識別される場合、更新することができる。

#### 【0023】

開発者は、スマートカードに（ユーザ）ライセンスを発行することができ、これらのライセンスは、記録の後にエンドユーザに送信され、あるいはライセンスは、スマートカードに又はTC PCのいずれかに電子的にダウンロードされることができる。データは、同時にダウンロードされることができ、又はおそらくCD-ROMのような非電子的な手段によって、独立して転送することができる。

#### 【0024】

##### 【発明の特定の実施形態】

さて、本発明の好適な実施形態を一例として説明する。

#### 【0025】

本発明の実施形態を説明する前に、信用される装置を組み込み（国際特許出願第PCT/GB00/00528号に記載されたように）、本発明の実施形態に

使用するために適したコンピューティングプラットフォームを、図1～図7に関連して説明する。また、コンピュータプラットフォームのユーザに対して個人的な信用されるトークン装置も、本発明の実施形態において使用するために適しているとして説明されており、好適な例において、このトークン装置は、スマートカードである。

#### 【0026】

説明されることは、物理的に信用される装置、又はモジュールのコンピューティングプラットフォームへの組み込みであり、その物理的に信用される装置又はモジュールの機能は、プラットフォームの完全性のメトリックスを提供し、それにより「信用されるプラットフォーム」を形成する確実に測定されたデータに対してプラットフォームのアイデンティティを結合することである。アイデンティティ及び完全性のメトリックスは、プラットフォームの信頼性を保証するために準備される信用される当事者(Trusted Party: TP)によって提供される予想される値と比較される。一致する場合、意味合い(implication)は、プラットフォームの少なくとも一部が完全性のメトリックスの範囲に応じて正確に動作していることである。

#### 【0027】

本明細書において、用語、「信用される(trusted)」は、物理的又は論理的なコンポーネントに関連して使用されたとき、物理的又は論理的なコンポーネントが常に予想された態様で動作することを意味するために使用される。コンポーネントの動作は、予測可能であり、既知である。信用されるコンポーネントは、無許可の修正に対して高度の抵抗力を有する。

#### 【0028】

本明細書において、用語、「コンピューティングプラットフォーム」(又は「コンピュータプラットフォーム」)は、少なくとも1つのデータプロセッサ、及び少なくとも1つのデータ記憶手段であるが、通常基本的に関連する通信設備を持たないもの、例えば複数のドライブ、関連するアプリケーション及びデータファイルを参照するために使用され、また、これは、例えばインターネットへの接続、外部ネットワークへの接続により、又はデータ記憶媒体、例えばCD-ROM、フロッ

ピーディスク（R）、リボンテープ等に記憶されたデータを受信することができる入力ポートを有することによって、外部のエンティティ、例えばユーザ又は別のコンピュータプラットフォームと相互作用可能であってもよい。

#### 【0029】

ユーザは、プラットフォームと他のデータを交換する前に、プラットフォームの正確な動作を確認する。ユーザは、信用される装置にそのアイデンティティ及び完全性のメトリックスを提供することをリクエストすることによって、これを行なう。（必要に応じて、信用される装置は、それ自体がプラットフォームの正確な動作を確認することができない場合、アイデンティティの証明を提供することを拒絶する。）ユーザは、アイデンティティ及び完全性のメトリックスの証明を受け取り、これらを真であると信じられる値と比較する。これらの適切な値は、ユーザによって信用されるTP又はその他のエンティティによって提供される。信用される装置によって報告されるデータが、TPによって提供されるものと同じである場合、ユーザは、プラットフォームを信用する。このことは、ユーザがエンティティを信用するためである。エンティティは、あらかじめアイデンティティを確認し、プラットフォームの適切な完全性のメトリックスを判定しているので、プラットフォームを信用する。

#### 【0030】

コンピューティングエンティティのユーザは、例えば、このような信用されるトークン装置の使用によって、コンピュータエンティティとの信用のレベルを確立することができる。信用されるトークン装置は、データ処理能力を有する個人の、及び携帯型の装置であり、この場合、ユーザは、高レベルの信用を有する。これは、ユーザを識別するために、信用されるプラットフォームによって使用されてもよい。信用されるトークン装置は、次の機能を実行することができる。すなわち、

- ・例えば、音声又はビジュアルディスプレイによってユーザに容易に分かる態様で、コンピューティングプラットフォームの正確な動作を確認すること、

- ・モニタリングコンポーネントが関連するコンピュータプラットフォームの正確な動作の証明を提供するためにモニタリングコンポーネントにチャレンジするこ

と、及び、

・モニタリングコンポーネントがコンピューティングエンティティの正確な動作の満足な証明を提供したかどうかに応じて、コンピューティングプラットフォームとトークン装置の相互作用のレベルを確立し、正確な動作のこのような証明がトークン装置によって受信されない場合、コンピュータエンティティとの特定の相互作用を制止すること。

#### 【0031】

一度ユーザが、プラットフォームの信用される動作を確立した場合、ユーザは、プラットフォームと他のデータを交換する。ローカルユーザに対して、交換は、プラットフォーム上で動作するある種のソフトウェアアプリケーションとの相互作用によるものであってもよい。リモートユーザに対して、交換は、セキュアトランザクションを含んでいてもよい。どちらにしても、交換されるデータは、信用される装置によって「サイン」されている。そして、ユーザは、動作を信用することができるプラットフォームとデータが交換されていることの一層大きな信用を有することができる。

#### 【0032】

信用される装置は、暗号プロセスを使用するが、これらの暗号プロセスのために外部インターフェースを必然的に設けるわけではない。また、もっとも望ましい具体化は、これらを他のプラットフォーム機能にアクセス不能にすることにより秘密を保護するために、及び無許可の修正に実質的に影響されない環境を提供するために、信用される装置に改竄防止策を施すことである。改竄防止は不可能なので、改竄に対する抵抗力を有する、又は改竄を検出する信用される装置が、最善の近似である。従って、信用される装置は、好適には改竄に対する抵抗力を有する1つの物理的なコンポーネントからなる。

#### 【0033】

改竄に対する抵抗力に関連する技術は、セキュリティーの技術における当業者によく知られている。これらの技術は、改竄に抵抗するための方法（信用される装置の適切なカプセル封入のような）、改竄を検出するための方法（信用される装置ケーシングにおける仕様電圧、X線又は物理的完全性の損失からの検出のよ



うな)、及び改竄が検出されたときにデータを除去するための方法を含む。適切な技術のそれ以上の議論は、<http://www.cl.cam.ac.uk/~mgk25/tamper.html>において見出すことができる。理解されるように、改竄防止が本発明のもっとも望ましい特徴であるとはいえ、本発明の通常の動作には入らず、かつ本発明の範囲を越えているようであり、すべての詳細において本明細書に記載しない。

#### 【0034】

信用される装置は、偽造することが困難でなければならないので、好適には物理的なものである。偽造が困難でなければならないので、もっとも好適には改竄に対する抵抗力を有する。信用される装置は、典型的にはローカル及び少し離れてアイデンティティを証明するために必要なので、暗号プロセスを使用することができるエンジンを含み、関連するプラットフォームのある種の完全性メトリックスを測定する少なくとも1つの方法を含む。

#### 【0035】

信用されるプラットフォーム10は、図1の線図において示される。プラットフォーム10は、キーボード14（これはユーザの確認鍵を提供する）、マウス16及びモニタ18の標準的な機能を含み、これらは、プラットフォームの物理的な「ユーザインターフェース」を提供する。信用されるプラットフォームのこの実施形態は、スマートカードリーダ12も含む。さらに後述するように、信用されるプラットフォームとの信用されるユーザの相互作用を可能にするためのスマートカード19が、スマートカードリーダ12の側面に沿って示される。プラットフォーム10において、複数のモジュール15が存在し、これらは、本質的にそのプラットフォームに適切な任意の種類の信用されるプラットフォームの他の機能要素である。このような要素の機能的な重要性は、本発明に関連せず、本明細書においてさらに議論しない。信用されるコンピュータエンティティの追加のコンポーネントは、典型的に1つ又は複数のローカルエリアネットワーク（LAN）ポート、1つ又は複数のモデムポート、及び1つ又は複数の電源、冷却ファン等を含む。

#### 【0036】

図2に示すように、信用されるコンピューティングプラットフォーム10のマザーボード20は、（その他の標準的なコンポーネントのなかで）主プロセッサ2

1、主メモリ22、信用される装置24、データバス26、及びそれぞれの制御ライン27及びライン28、プラットフォーム10のためのBIOSプログラムを含むBIOSメモリ29、及び入力/出力(I/O)装置23を含み、この入力/出力装置は、マザーボードのコンポーネントと、スマートカードリーダー12、キーボード14、マウス16及びモニタ18(及びモデム、プリンタ、スキャナ等のような任意の追加の周辺装置)との間の相互作用を制御する。主メモリ22は、典型的にはランダムアクセスメモリ(RAM)である。動作中、プラットフォーム10は、オペレーティングシステム、例えばウインドウズNT(R)をハードディスク(図示せず)からRAMへロードする。さらに、動作中、プラットフォーム10は、プラットフォーム10によって実行することができるプロセス又はアプリケーションをハードディスク(図示せず)からRAMへロードする。

#### 【0037】

コンピュータエンティティは、論理的及び物理的なアーキテクチャを有するものと考えることができる。論理的なアーキテクチャは、本明細書の図1～図4に記載された物理的なアーキテクチャと共に存在するものと同じ基本的な部分を、コンピュータプラットフォームと信用されるコンポーネントとの間に有する。すなわち、信用されるコンポーネントは、物理的に関連するコンピュータプラットフォームとは論理的に異なっている。コンピュータのエンティティは、コンピュータプラットフォームに物理的に常駐する論理空間であるユーザ空間(第1のプロセッサ及び第1のデータ記憶手段)、及び信用されるコンポーネントに物理的に常駐する論理空間である信用されるコンポーネントの空間からなる。ユーザ空間には、1つ又は複数のドライバ、1つ又は複数のアプリケーションプログラム、ファイル記憶領域、スマートカードリーダー、スマートカードインターフェース、及びユーザ空間における動作を実行でき、信用されるコンポーネントに報告を返すことができるソフトウェアエージェントがある。信用されるコンポーネントの空間は、信用されるコンポーネントに基づき、かつそこに物理的に常駐する論理領域であり、信用されるコンポーネントの第2のデータプロセッサ及び第2のメモリ領域によって支援される。モニタ18は、信用されるコンポーネントの空間から画像を直接受信する。コンピュータエンティティの外部に、外部通信ネットワー

ク、例えばインターネット、及び種々のローカルエリアネットワーク、ドライバ（これは1つ又は複数のモデムポートを含むことができる）を介してユーザ空間に接続される広範囲ネットワークがある。外部のユーザのスマートカードは、ユーザ空間におけるスマートカードリーダー内に入力される。

#### 【0038】

一般に、パーソナルコンピュータにおいて、BIOSプログラムは、特別に予約されたメモリ領域内に配置されており、第1のメガバイトの上側の64Kは、システムメモリをなし（アドレスF000h～FFFFh）、主プロセッサは、業界全体の標準にしたがって、初めにこのメモリ位置を見るように構成される。

#### 【0039】

本プラットフォームと従来のプラットフォームとの間の重要な相違は、リセットの後に、主プロセッサが初めに信用される装置によって制御され、次いで、この装置が制御をプラットフォームに特有のBIOSプログラムに引き渡し、次いで、このプログラムが、通常のようにすべての入力／出力装置を初期設定することである。BIOSプログラムが実行された後に、制御は、通常のようにBIOSプログラムによってウインドウズNT（R）のようなオペレーティングシステムプログラムに引き渡され、このOSは、一般にハードディスクドライブ（図示せず）から主メモリ22へロードされる。

#### 【0040】

明らかに通常の手順からのこの変更は、業界基準の具体化に対する修正を必要とし、それにより主プロセッサ21は、その第1の命令を受信するために信用される装置24をアドレス指定するように命令される。この変更は、主プロセッサ21への異なったアドレスをハードコーディング（hard-coding）することによって簡単に行なうことができる。代案として、信用される装置24に、標準BIOSプログラムアドレスを割り当てることができ、この場合、主プロセッサの構成を修正する必要はない。

#### 【0041】

BIOSブートブロックが、信用される装置24内に含まれることは、おおいに望ましい。このことは、完全性メトリックスの取得の破壊（このことは、不良

なソフトウェアプロセスが存在する場合に、違った風に起こるかもしれない)を防止し、BIOSが(正確な場合でさえ)オペレーティングシステムのために適切な環境を構築することに失敗する状況を作り出す不良なソフトウェアプロセスを防止する。

#### 【0042】

説明すべき好適な実施形態において、信用される装置24が単一の別個のコンポーネントであるとはいえ、信用される装置24の機能が、代わりにマザーボード上の複数の装置に分割されることができ、又はプラットフォームの既存の標準的な1つ又は複数の装置内に統合さえできることが企図される。例えば、機能及びそれらの通信が破壊できないとすれば、信用される装置の1つ又は複数の機能を主プロセッサ自体内に統合することは実現可能である。しかしながら、このことは、おそらく信用される機能による単独の使用のためにプロセッサにおける分離したリード線を必要とするであろう。追加の、又は代案として、本実施形態において信用される装置は、マザーボード20内に統合するように適合されたハードウェア装置であるとはいえ、信用される装置が、必要であればプラットフォームに取り付けることができる dongle のような「移動可能な」装置として実施できることが予想される。信用される装置が統合されるか、又は移動可能であるかどうかは、設計上の選択事項である。しかし信用される装置が分離可能である場合、信用される装置とプラットフォームとの間の論理結合を提供するための機構が存在しなくてはならない。

#### 【0043】

信用される装置24は、図3に示すように、多数のブロックを含む。システムをリセットした後、信用される装置24は、プラットフォーム10(システムクロック及びモニタ上のディスプレイを含む)のオペレーティングシステムが適正にセキュアの状態に走っていることを保証するために、セキュアブートプロセスを実行する。セキュアブートプロセスの間に、信用される装置24は、コンピューティングプラットフォーム10の完全性のメトリックスを取得する。信用される装置24は、セキュアデータ伝送、及び例えば暗号化/暗号解読及びサイン/証明を介してスマートカードと信用される装置24との間の認証も行なうことができ

る。信用される装置24は、ユーザインターフェースのロックのような種々のセキュリティ制御ポリシーを安全に強制することもできる。

#### 【0044】

特に、信用される装置24は、信用される装置24の全体的な動作を制御し、信用される装置24の他の機能及びマザーボード20上の他の装置と相互作用するようにプログラミングされたコントローラ30、プラットフォーム10から完全性のメトリックスを取得するための測定機能31、特定のデータにサインし、暗号化し又は暗号解読するための暗号機能32、スマートカードを認証するための認証機能33、及びマザーボード20のデータバス26、制御ライン27及びアドレスライン28に信用される装置24をそれぞれ接続するための適切なポート(36、37&38)を有するインターフェース回路34を含む。信用される装置24におけるそれぞれのブロックは、(一般に、コントローラ30を介して)信用される装置24の適切な揮発性メモリ領域4及び/又は不揮発性メモリ領域3にアクセスする。さらに、信用される装置24は、既知の態様で改竄に対する抵抗力を有するように設計される。

#### 【0045】

性能の理由で、信用される装置24は、特定用途向け集積回路(ASIC)として実現することができる。しかしながら、融通性のため、信用される装置24は、好適には適切にプログラミングされたマイクロコントローラである。ASIC及びマイクロコントローラは、両方ともマイクロエレクトロニクスの分野においてよく知られており、本明細書においてさらに詳細に考察しない。

#### 【0046】

信用される装置24の不揮発性メモリ3に記憶されるデータの1つの項目は、証明350である。証明350は、信用される装置24の少なくとも公開鍵351、及び信用される当事者(TP)によって測定されたプラットフォーム完全性のメトリックスの認証された値352を含む。証明350は、信用される装置24内に記憶される前に、TPの秘密鍵を使用してTPによってサインされる。後の通信のセッション中に、プラットフォーム10のユーザは、認証された完全性のメトリックス352と取得された完全性のメトリックスを比較することによって、

プラットフォーム10の完全性を確認することができる。一致する場合、ユーザは、プラットフォーム10が破壊されていないことを確信することができる。TPの一般に使用できる公開鍵の情報は、証明350の簡単な検証を可能にする。不揮発性メモリ35も、アイデンティティ(ID)ラベル353を含む。IDラベル353は、従来のIDラベル、例えば連続番号であり、このIDラベルは、ある種の状況内において一意である。IDラベル353は、信用される装置24に関連するデータに索引付け及びラベル付けのために一般に使用されるが、信用される状態下においてプラットフォーム10のアイデンティティを証明するためには、それ自体不十分である。

#### 【0047】

信用される装置24は、関連するコンピューティングプラットフォーム10の完全性のメトリックスを確実に測定し又は取得する少なくとも1つの方法を備える。本実施形態において、完全性のメトリックスは、BIOSメモリにおけるBIOS命令の要約を発生することによって、測定機能31によって取得される。このような取得された完全性のメトリックスは、前記のように確認された場合、プラットフォーム10の潜在的なユーザに、プラットフォーム10がハードウェアレベル又はBIOSプログラムレベルにおいて破壊されていないという高レベルの信用を与える。他の既知のプロセス、例えばウイルスチェッカは、一般にオペレーティングシステム及びアプリケーションプログラムコードが破壊されていないことをチェックする立場にある。

#### 【0048】

測定機能31は、信用される装置24のハッシュプログラム354及び秘密鍵355を記憶するための不揮発性メモリ3、及び要約361の形態で取得された完全性のメトリックスを記憶するための揮発性メモリ4にアクセスする。適切な実施形態において、揮発性メモリ4は、プラットフォーム10にアクセスするために使用されることができる1つ又は複数の認証されたスマートカード19の公開鍵及び関連するIDラベル360a-360nを記憶するために使用されてもよい。

#### 【0049】

1つの好適な実施形態において、要約(digest)、並びに完全性のメトリックスは、ブール値を含み、このブール値は、明らかになるであろう理由のために、測定機能31によって揮発性メモリ4に記憶されている。

#### 【0050】

図4に関連して、今度は完全性のメトリックスを取得するための好適なプロセスを説明する。

#### 【0051】

ステップ400において、スイッチオンで、測定機能31は、信用される装置24がアクセスされた第1のメモリであるかどうかを判定するために、データに対する主プロセッサ21の活動、制御及びアドレスライン(26、27&28)をモニタする。従来の動作において、主プロセッサは、第1にBIOSプログラムを実行するために第1にBIOSメモリに命令される。しかしながら、本実施形態によれば、主プロセッサ21は、メモリとして働く信用される装置24に命令される。ステップ405において、信用される装置24がアクセスされる第1のメモリである場合、ステップ410において、測定機能31は、不揮発性メモリ3にブール値を書き込み、このブール値は、信用される装置24がアクセスされる第1のメモリであったことを示す。そうでなければ、ステップ415において、測定機能は、ブール値を書き込み、このブール値は、信用される装置24がアクセスされる第1のメモリではなかったことを示す。

#### 【0052】

信用される装置24が第1にアクセスされるものでない場合、もちろん信用される装置24が全くアクセスされない可能性が存在する。このことは、例えば主プロセッサ21が第1にBIOSプログラムを走らせるように操作された場合である。これらの状況下で、プラットフォームは、動作するが、完全性のメトリックスが利用できないので、要求に応じてその完全性を確認することはできない。さらに、BIOSプログラムがアクセスされた後、信用される装置24がアクセスされる場合、ブール値は、プラットフォームの完全性の不足を明確に示す。

#### 【0053】

ステップ420において、主プロセッサ21によってメモリとしてアクセスさ

れたとき（又は場合）、主プロセッサ21は、ステップ425において、測定機能31から記憶された固有のハッシュ命令354を読取る。ハッシュ命令354は、主プロセッサ21による処理のためにデータバス26を介して渡される。ステップ430において、主プロセッサ21は、ハッシュ命令354を実行してこれらを使用し、ステップ435において、BIOSメモリ29の内容を読取り、ハッシュプログラムにしたがってこれらの内容を処理することによって、BIOSメモリ29の要約を計算する。ステップ440において、主プロセッサ21は、信用される装置24における適切な不揮発性メモリ記憶位置4に計算された要約361を書き込む。次いで、ステップ445において、測定機能31は、BIOSメモリ29におけるBIOSプログラムを呼び出し、従来の態様で実行を継続する。

#### 【0054】

明らかに、必要な信用の範囲に応じて、完全性のメトリックスを計算することができる多数の異なった態様が存在する。BIOSプログラムの完全性の測定は、プラットフォームの基礎をなすプロセス環境の完全性に対する基本的なチェックを提供する。完全性のメトリックスは、ブートプロセスの妥当性に関して推論を可能にするこのような形態からなり、完全性のメトリックスの値は、プラットフォームが正確なBIOSを使用してブートされるかどうかを確認するために使用することができる。必要に応じて、BIOS内の個々の機能ブロックは、これらのブロック自体の要約値を有することができ、全体的なBIOSの要約は、これらの個々の要約からなる要約である。このことは、BIOS動作のどの部分が意図した目的に対して重要であるか、及びどれが不適切であるか（この場合、個々の要約は、ポリシーのもとに動作の妥当性が確立できるように記憶されなければならない）を示すためにポリシーをイネーブルにする。

#### 【0055】

他の完全性のチェックは、プラットフォームに取り付けられた種々の他のデバイス、コンポーネント又は装置が存在し、正確な動作順序にあることを確立することを含むことができる。1つの例において、SCSIコントローラに関連するBIOSプログラムは、周辺装置との通信が信頼できることを保証するために確認



することができる。別の例において、プラットフォーム上の他の装置、例えばメモリ装置又はコプロセッサの完全性は、一貫した結果を保証するために固定のチャレンジ/レスポンスの相互作用を規定することによって、確認されることができる。信用される装置24が分離できるコンポーネントである場合、相互作用のある種のこのような形態は、信用される装置24とプラットフォームとの間の適切な論理結合を提供するために望ましい。また、本実施形態において、信用される装置24は、プラットフォームの他の部分と通信するその主な手段としてデータベースも使用し、実現可能であるとはいえ、それほど便利ではないが、配線による経路又は光学経路のような代わりの通信経路を設けることは可能である。さらに、本実施形態において、信用される装置24は、完全性のメトリックスを計算するように主プロセッサ21に命令するとはいえ、他の実施形態において、信用される装置自体が1つ又は複数の完全性のメトリックスを測定するように構成されることは予想される。

#### 【0056】

好適には、BIOSブートプロセスは、ブートプロセス自体の完全性を確認するための機構を含む。このような機構は、例えばIntelの草案「Wired For Management baseline specification v2.0-B00T Integrity Service」からすでに知られており、ソフトウェア又はファームウェアをローディングする前に、そのソフトウェア又はファームウェアの要約を計算することを含む。このような計算された要約は、信用されるエンティティによって提供される証明に記憶された値と比較され、その公開鍵は、BIOSにとって既知である。次いで、ソフトウェア／ファームウェアは、計算された値が証明から予想された値と一致した場合にだけロードされ、証明は、信用されるエンティティの公開鍵の使用によって有効と証明されている。そうでなければ、適切な例外取り扱いルーチンが呼び出される。

#### 【0057】

必要に応じて、計算されたBIOSの要約を受信した後、信用される装置24は、証明におけるBIOS要約の適切な値を検査することができ、計算された要約が適切な値と一致しない場合、BIOSに制御を渡さない。追加の、又は代案

として、信用される装置24は、プール値を検査することができ、信用される装置24がアクセスされる第1のメモリではない場合、BIOSに制御を戻さない。これらのいずれの場合にも、適切な例外取り扱いルーチンを呼び出すことができる。

#### 【0058】

図5は、TP、プラットフォームに組み込まれた信用される装置24、及び信用されるプラットフォームの完全性を確認したいユーザ（リモートプラットフォームの）による動作のフローを示す。ユーザがローカルユーザである場合、図5に示されたものと実質的に同じステップが含まれていることが認められる。どちらにしても、ユーザは、一般に検証を実行するためにソフトウェアアプリケーションのある種の形態を信用する。リモートプラットフォーム又は信用されるプラットフォーム上でソフトウェアアプリケーションを走らせることは可能である。しかしながら、リモートプラットフォーム上でさえ、ソフトウェアアプリケーションが何らかの方法で破壊され得る可能性が存在する。従って、高レベルの完全性に対して、ソフトウェアアプリケーションがユーザのスマートカード上に常駐し、このユーザが、検証のために適切なリーダにスマートカードを挿入することは好適である。特定の実施形態は、このような構成に関係する。

#### 【0059】

第1の例において、信用されるプラットフォームを保証するTPは、これを保証するか又はしないかどうかを決めるために、プラットフォームのタイプを検査する。これはポリシーの問題であろう。すべてが良好ならば、ステップ500において、TPは、プラットフォームの完全性メトリックスの値を測定する。次いで、TPは、ステップ505において、プラットフォームに対して証明を生成する。証明は、測定された完全性のメトリックスに信用される装置の公開鍵及び必要に応じてそのIDラベルを添付することによって、及びTPの秘密鍵を有するストリングにサインすることによって、TPによって生成される。

#### 【0060】

信用される装置24は、ユーザから受信されるいくつかの入力データを処理するためにその秘密鍵を使用することによってそのアイデンティティを結果として

証明することができ、入力／出力対が秘密鍵の情報なしでは統計的に生成することができないように、出力データを生成することができる。従って、秘密鍵の情報は、この場合に、アイデンティティの基礎を形成する。明らかに、アイデンティティの基礎を形成するために、対称の暗号化を使用することが適している。しかしながら、対称の暗号化の使用の欠点は、ユーザがユーザの秘密を信用される装置と共有する必要があるという点にある。さらに、ユーザと秘密を共有する必要の結果として、対称の暗号化は、原則的にユーザにアイデンティティを証明するのに十分であるが、信用される装置又はユーザから発する証明を完全に確信することができない第三者にアイデンティティを証明することは不十分である。

#### 【0061】

ステップ510において、信用される装置24は、信用される装置24の適切な不揮発性メモリ記憶位置3へ証明350を書き込むことによって、初期化される。このことは、好適にはマザーボード20にインストールされた後に、信用される装置24とのセキュア通信によって行なわれる。信用される装置24に証明を書き込む方法は、秘密鍵を書き込むことによってスマートカードを初期設定するために使用される方法と類似している。セキュア通信は、TPだけに知られた「マスター鍵」によって支援され、これは、製造の間に信用される装置（又はスマートカード）に書き込まれ、信用される装置24にデータを書き込むことを可能にするために使用され、マスター鍵の情報なしでの信用される装置24へのデータの書き込みは不可能である。

#### 【0062】

プラットホームの動作中のいくつかの後の点において、例えばスイッチオンされ又はリセットされたとき、ステップ515において、信用される装置24は、プラットホームの完全性のメトリックス361を取得して記憶する。

#### 【0063】

ユーザがプラットホームと通信することを望むとき、ステップ520において、ユーザは、乱数のようなナンス（nonce：その時限りの数）を作成し、ステップ525において、信用される装置24にチャレンジする（プラットホームのオペレーティングシステム又は適切なソフトウェアアプリケーションは、チャレン

ジを認識し、これを一般にBIOSタイプの呼び出しを介して適切な様式で信用される装置24に渡すように構成されている)。ナンスを用いて、信用できないプラットフォームによって古いが本物のサインの再生(「再生攻撃」と称する)によって欺かれることからユーザを保護する。ナンスを提供し、レスポンスを確認するプロセスは、よく知られた「チャレンジ/レスポンス」プロセスの例である。

#### 【0064】

ステップ530において、信用される装置24は、チャレンジを受信し、適切なレスポンス(応答)を生成する。これは、測定された完全性のメトリックス及びナンスの要約、及び必要に応じてそのIDラベルであってもよい。次いで、ステップ535において、信用される装置24は、その秘密鍵を使用して、要約にサインし、証明350が添付されたサイン済みの要約をユーザに返送する。

#### 【0065】

ステップ540において、ユーザは、チャレンジ・レスポンスを受信し、かつTPの周知の公開鍵を使用して証明を確認する。次いで、ユーザは、ステップ550において、証明から信用される装置24の公開鍵を抽出し、これをチャレンジ・レスポンスからサインされた要約を暗号解読するために使用する。次いで、ステップ560において、ユーザは、チャレンジ・レスポンス内のナンスを確認する。次にステップ570において、ユーザは、チャレンジ・レスポンスから抽出した計算された完全性のメトリックスを、証明から抽出した適切なプラットフォームの完全性のメトリックスと比較する。前述の検証ステップのいずれかが、ステップ545、555、565又は575において失敗した場合、すべてのプロセスは、それ以上の通信を行なうことなく、ステップ580において終了する。

#### 【0066】

すべてが良好であると仮定すれば、ステップ585及び590において、ユーザと信用されるプラットフォームは、他のデータのためのセキュア通信をセットアップするために他のプロトコルを使用し、この場合、プラットフォームからのデータは、好適には信用される装置24によってサインされる。

#### 【0067】

この検証プロセスのさらなる洗練が可能である。チャレンジャ（チャレンジの送信側）は、チャレンジを介して、プラットフォームの完全性メトリックスの値及びこれを得る方法の両方に気付くことが望ましい。情報のこれらの部分の両方は、チャレンジャがプラットフォームの完全性に関する適切な判断を行なうことができるようにするために望ましい。チャレンジャは、使用可能な多数の異なったオプションも有し、完全性のメトリックスが信用される装置24において有効と認められることを受け入れることができ、又は代案として完全性のメトリックスの値がチャレンジャによって保持された値に等しい場合、プラットフォームが完全性の関連するレベルを有することだけを受け入れることができる（又はこれら2つの場合に信用の異なったレベルであることをそこに保持することができる）。

【0068】

証明及びチャレンジ／レスポンスを使用して、及びこれらをアイデンティティを証明するために使用して、サインする技術は、セキュリティの分野の当業者によく知られており、従って、本明細書においてさらに詳細に説明する必要がない。

【0069】

ユーザのスマートカード19は、コンピューティングエンティティから分離したトークン装置であり、この装置は、スマートカードリーダポート19を介してコンピューティングエンティティと相互作用する。ユーザは、いくつかの異なった販売者又はサービスプロバイダによって発行されたいくつかの異なったスマートカードを有することができ、信用されるコンポーネント及びスマートカードリーダを備えた、本明細書で説明したような複数のコンピューティングエンティティのうちのいずれか1つからインターネット又は複数のネットワークコンピュータにアクセスすることができる。ユーザが使用している個々のコンピューティングエンティティにおけるユーザの信用は、ユーザの信用されるスマートカードトークンとコンピューティングエンティティの信用されるコンポーネントとの間の相互作用から発する。ユーザは、信用されるコンポーネントの信頼性を確認するためにそれらの信用されるスマートカードトークンを信用する。

【0070】

ユーザのスマートカード19の処理部分60は、図6に示される。図示されたように、ユーザのスマートカード19の処理部分60は、プロセッサ61、メモリ62及びインターフェース接触部63の標準的な特徴を有する。プロセッサ61は、後に説明するように、ユーザスマートカード19の認証及びプラットフォーム10の検証を伴う簡単なチャレンジ/レスポンス動作のためにプログラミングされている。メモリ62は、その秘密鍵620、その公開鍵628、（必要に応じて）ユーザプロファイル621、TPの公開鍵622及びアイデンティティ627を含む。ユーザプロファイル621は、ユーザによって使用可能な許容できる補助のスマートカード20 AC1-ACn、及びユーザのための個々のセキュリティポリシー624を記述する。それぞれの補助スマートカード20に対して、ユーザプロファイルは、それぞれの識別情報623、スマートカード（1つが存在する場合）間の信用構造625、及び必要に応じてスマートカードのタイプ又は形式626を含む。

#### 【0071】

ユーザプロファイル621において、それぞれの補助スマートカード20のエントリーAC1-ACnは、関連する識別情報623を含み、この情報は、カードのタイプに応じて変化する。例えば、キャッシュカードに対する識別情報は、一般に簡単な一連番号を含むが、それに対して、暗号カードについては、識別情報は、一般に暗号カードの公開鍵（又は証明）を含む（秘密鍵は、暗号カード自体に秘密に記憶されている）。

#### 【0072】

「セキュリティポリシー」624は、補助スマートカード20を使用する間に、プラットフォーム10上でユーザが有する許諾を命令する。例えば、ユーザインターフェースは、補助スマートカード20の機能に依存して、補助スマートカード20が使用中である間に、ロック可能又はロック解除可能である。追加の、又は代案として、プラットフォーム10上の所定のファイル又は実行可能なプログラムは、特定の補助スマートカード20がどのように信用されたかに依存して、アクセス可能又は不可能にすることができる。さらにセキュリティポリシー624は、後に説明するように、「クレジット受領」又は「一時的な委任」のよう

な補助スマートカード20に対する特定の動作のモードを指定することができる。

#### 【0073】

「信用構造」625は、補助スマートカード20が、それ自体ユーザスマートカード19を第1に再使用することなく、システム内にさらなる補助スマートカード20を「導入」することができるかどうかを定義する。ここに詳細に説明した実施形態において、定義されただけの信用構造は、ユーザスマートカード19とユーザスマートカード19によってプラットフォーム10に導入できる補助スマートカード20との間にある。導入は、後に説明するように、「単一セッション」又は「複数のセッション」とすることができる。しかしながら、所定の補助スマートカード20が、さらなる補助スマートカード20を実際に導入することができない理由は存在しない。このことは、補助スマートカード20が、導入することができるその又はそれぞれの補助スマートカードを記述するユーザプロファイルの均等物を有することを必要とする。

#### 【0074】

補助スマートカード20の使用は、本発明の必須の特徴ではなく、本出願においてさらに説明されていない。補助スマートカードの使用は、2000年3月5日に出願され、「Computing Apparatus and Method of Operating Computing Apparatus」と題する本出願人の同時係属国際特許出願第PCT/GB00/00751号明細書の主題であり、これは、参照により本明細書に組み込まれる。

#### 【0075】

今度は、図7におけるフロー線図に関連してユーザスマートカード19とプラットフォーム10との間の認証のための好適なプロセスを説明する。説明するように、プロセスは、便宜的にチャレンジ/レスポンスのルーチンを実行する。多数の使用可能なチャレンジ/レスポンスの機構が存在する。本実施形態において使用される認証プロトコルの具体化は、ISO/IEC 9798-3に記載されたような相互（又は3ステップの）認証である。もちろん、他の認証手続き、例えばISO/IEC 9798-3にも記載されたような2ステップ、又は4ステップを使用することができない理由は存在しない。

## 【0076】

初めにユーザは、ステップ700において、ユーザのユーザスマートカード19をプラットフォーム10のスマートカードリーダ12へ挿入する。あらかじめプラットフォーム10は、一般にその標準オペレーティングシステムの制御のもとで動作して、認証プロセスを実行し、この認証プロセスは、ユーザのユーザスマートカード19をユーザが挿入することを待っている。このように、アクティヴとなるスマートカードリーダ12から離れて、プラットフォーム10は、一般にユーザインターフェース（すなわちスクリーン、キーボード及びマウス）を「ロックすること」によってユーザをアクセス不能にする。

## 【0077】

ユーザスマートカード19をスマートカードリーダ12へ挿入する場合、信用される装置24は、ステップ705において、ユーザスマートカード19にナンスAを生成して送信することによって、ステップにおいて相互認証を試みることをトリガする。乱数のようなナンスは、信用できない第三者によって古いが本物のレスポンスの再生（「再生攻撃」と称する）によって引き起こされる欺きから発信者（originator）を保護するために使用される。

## 【0078】

レスポンスに関して、ステップ710において、ユーザスマートカード19は、以下の連鎖を含むレスポンスを生成して返送する。すなわち、ナンスAの平易なテキスト、ユーザスマートカード19により生成される新しいナンスB、信用される装置24のID353及びある種の冗長性；ユーザスマートカード19の秘密鍵で平易なテキストにサインすることによって生成された平易なテキストのサイン；及びユーザスマートカード19のID及び公開鍵を含む証明。

## 【0079】

信用される装置24は、ステップ715において、平易なテキストのサインを確認するために証明内の公開鍵を使用することによって、レスポンスを認証する。レスポンスが認証されない場合、ステップ720において、プロセスは終了する。レスポンスが認証される場合、ステップ725において、信用される装置24は、以下の連鎖を含む別のレスポンスを生成して送信する。すなわち、ナンス



Aの平易なテキスト、ナンスB、ユーザスマートカード19のID627及び取得された完全性のメトリックス；信用される装置24の秘密鍵を使用して平易なテキストにサインすることによって生成された平易なテキストのサイン；及び信用される装置24の公開鍵及び認証された完全性のメトリックス（どちらもTPの秘密鍵によってサインされた）を含む証明。

#### 【0080】

ユーザスマートカード19は、TPの公開鍵を使用することにより、及び取得された完全性のメトリックスを認証された完全性のメトリックスと比較することにより、このレスポンスを認証し、この場合、ステップ730において、一致は、成功した検証を示す。さらなるレスポンスが認証されない場合、ステップ735において、プロセスは終了する。

#### 【0081】

手続きが成功した場合、信用される装置24はユーザスマートカード19を認証しており、かつユーザスマートカード19は信用されるプラットフォーム10の完全性を確認しており、ステップ740において、認証プロセスは、ユーザのためのセキュアプロセスを実行する。次いで、ステップ745において、認証プロセスは、インタバルタイマをセットする。その後、ステップ750において、適切なオペレーティング割り込みルーチンを使用して、認証プロセスは、タイマがいつ所定のタイムアウト期間を満たすか、又は超えるかを検出するために、周期的にインタバルタイマを処理する。

#### 【0082】

明らかに認証プロセス及びインタバルタイマは、セキュアプロセスと共に並行して走る。タイムアウト期間を満たし、又は超えた場合、ステップ760において、ユーザスマートカード19自体を識別するためにユーザスマートカード19のチャレンジを送信することによって、認証プロセスは、ユーザスマートカード19を再認証するために信用される装置24をトリガする。ステップ765において、ユーザスマートカード19は、そのID627及びその公開鍵628を含む証明を返送する。ステップ770において、レスポンスがなかった場合（例えば、ユーザスマートカード19が取り外されている結果として）、又は証明がも

はや何らかの理由のために有効でなかった場合（例えば、ユーザスマートカードが異なったスマートカードに置き換えられている）、ステップ775において、セッションは、信用される装置24によって終了される。そうでなければ、ステップ770において、ステップ745からのプロセスが、インタバルタイマのリセットにより繰り返される。

### 【0083】

証明及びチャレンジ／レスポンスを使用して、及びアイデンティティを証明するためにこれらを使用するサインの技術は、セキュリティの分野の当業者によく知られており、従って、本明細書においてさらに詳細に説明しない。

### 【0084】

今度は、図21及び図8～図13を参照して、2000年2月15日に出願された国際特許出願第PCT/GB00/00504号の主題であるシステムの特定の実施形態を説明する。このシステムは、本発明の用途に特に適している。図21において、ホストコンピュータ100は、主CPU102、ハードディスクドライブ104、PCIネットワークインターフェースカード106及びDRAMメモリ108を有し、従来の（「通常の」）通信経路110（ISA、EISA、PCI、USBのような）をそれらの間に備える。ネットワークインターフェースカード106は、ホストコンピュータ100の外側の世界との外部通信経路112も有する。

### 【0085】

ネットワークインターフェースカード106は、その間にインターフェース118を備えた「赤」及び「黒」データゾーン114、116に論理的に分割されている。赤ゾーン114において、データは、通常平易なテキストであり、検出不可能な変更及び望ましくない盗聴（eavesdropping）に弱くて無防備である。黒データゾーン116において、データは検出不可能な変更及び望ましくない盗聴から保護されている（好適には標準的な暗号機構によって暗号化される）。インターフェース118は、赤情報が黒ゾーン116に漏れないことを確実にする。インターフェース118は、好適には赤及び黒ゾーン114、116を分離するために、標準的な暗号方法及び電子分離技術を使用する。このような赤及び黒

ゾーン114、116及びインターフェース118の設計及び構成は、セキュリティー及び電子の、特に軍事分野における当業者によく知られている。通常の通信経路110及び外部通信経路112は、ネットワークインターフェースカード106の黒ゾーン116に接続される。

#### 【0086】

ホストコンピュータ100は、信用されるモジュール120も含み、このモジュール120は、通常の通信経路110のみならず、相互に分離した追加の通信経路122（補助参照符号122a、122b、122c）にもより、CPU102、ハードディスクドライブ104及びネットワークインターフェースカード106の赤ゾーン114に接続される。一例として、信用されるモジュール120は、メモリ108とのこのような分離した追加の通信経路122を持たない。

#### 【0087】

信用されるモジュール120は、それぞれ追加の通信経路122a、122b、122cを介して、CPU102、ハードディスクドライブ104及びネットワークインターフェースカード106の赤ゾーン114と通信できる。信用されるモジュール120は、通常の通信経路110を介して、CPU102、ハードディスクドライブ104、ネットワークインターフェースカード106の黒ゾーン116及びメモリ108とも通信できる。信用されるモジュール120は、信用されるモジュールに記憶されたポリシーの制御のもとで、信用されるモジュール120及び追加の通信経路122を介して、CPU102、ハードディスクドライブ104及びネットワークインターフェースカード106の赤ゾーン114の間の所定情報を経路指定するために、100VGスイッチングセンタとして働くこともできる。信用されるモジュール120は、暗号鍵を生成することもでき、それぞれ追加の通信経路122a、122b、122cを介して、これらの鍵をCPU102、ハードディスクドライブ104及びネットワークインターフェースカード106の赤ゾーン114に分配することもできる。

#### 【0088】

図8は、信用されるモジュール120の物理的なアーキテクチャを示す。第1のスイッチングエンジン124は、追加の通信経路122a、122b、122

cに独立して接続され、信用されるモジュール120の内部通信経路126にも接続される。このスイッチングエンジン124は、ポリシーの制御のもとで、信用されるモジュール120へロードされる。信用されるモジュール120の他のコンポーネントは次のとおりである：

- ・信用されるモジュール120を管理し、信用されるモジュール120のための汎用コンピューティングを実行するコンピューティングエンジン128、
- ・一時的なデータを記憶する揮発性メモリ130、
- ・長期にデータを記憶する不揮発性メモリ132、
- ・暗号化及び鍵生成のようなスペシャリスト暗号機能を実行する暗号エンジン134、
- ・暗号動作に主として使用される乱数源136、
- ・通常の通信経路110に信用されるモジュール120を接続する第2のスイッチングエンジン138、及び
- ・改竄検出機構140、

これらすべては、信用されるモジュール120の内部通信経路126に接続される。

#### 【0089】

信用されるモジュール120は、図1～図7に関連してさらに詳細に前述したように、信用される装置又はモジュール24に基づいている。

#### 【0090】

暗号鍵生成及び分配に関して、信用されるモジュール120は、乱数発生器136、ハッシュアルゴリズム及び他のアルゴリズムを使用して、暗号鍵を生成し、これらすべては、セキュリティの分野の当業者に、それ自体周知である。信用されるモジュール120は、通常の通信経路110というよりむしろそれぞれ追加の通信経路122a、122b、122cを使用して、CPU102、ハードディスクドライブ104及びネットワークインターフェースカード106の赤ゾーン114に選択された鍵を分配する。鍵は、通常の通信経路110を介してプラットフォームの内部モジュール102、104、106、120間の通信用に使用してもよい。他の一時的な鍵は、信用されるモジュール120の外側に漏ら

してはいけない長期のアイデンティティの秘密を使用するSSL初期接続手順段階を信用されるモジュール120が完了した後に、SSLプロトコルを使用して外部データのバルク暗号化又は暗号解読のために使用することができる（ネットワークインターフェースカード106又はCPU102により）。他の一時的な鍵は、信用されるモジュール120の外側に漏らしてはいけない長期の秘密を使用して信用されるモジュール120の内部でこれらの一時的な鍵が作成され又は露呈された後、ハードディスクドライブ104に記憶されたデータのバルク暗号化又は暗号解読のために使用することができる（ハードディスクドライブ104又はCPU102により）。

#### 【0091】

信用されるモジュール120は、暗号鍵の選択的な分配によってモジュール間の通信に関するポリシー制御を実施する。信用されるモジュール120は、任意のモジュール対の間で共有のインフラストラクチャ110を介したセキュア通信を可能にする鍵の発行を拒絶することによって、これらのモジュール対の間の通信にポリシーの禁止を実施する。

#### 【0092】

図9は、信用されるモジュール120が、ウォッチドッグ機能、及び追加の通信経路122に接続されたモジュール102、104、106の「ピング（ping）」を行なうことができるプロセスを示す。信用されるモジュールは、チャレンジ142を生成し、それぞれ追加の通信経路122a、122b、122cを使用して、チャレンジ142をCPU102、ハードディスクドライブ104及びネットワークインターフェースカード106の赤ゾーン114に送信する。CPU102、ハードディスクドライブ104及びネットワークインターフェースカード106のそれぞれは、それぞれのモジュールがアクティブであるかどうか、及び好適にはモジュールが適正に動作していることを伝えるために、それぞれの追加の通信経路122a、122b、122c上の、それぞれのレスポンス144a、144b、144cによって応答する。信用されるモジュール120は、レスポンス144a、144b、144cを記録し、これらを、図1～図7に関連して前述した完全性のチャレンジに対するそのレスポンスにおけるメトリクス

として使用する。

### 【0093】

図10は、信用されるモジュール120が暗号能力を有するプラットフォーム内の唯一のモジュールである場合、到来する外部セキュアメッセージを処理するプロセスを示す。外部メッセージ146は、外部通信経路112を使用して、ネットワークインターフェースカード106の黒ゾーン116によって受信される。ネットワークインターフェースカード106は、通常の通信経路110を使用して、信用されるモジュール120に、何らかのデータ及び認証及び完全性チェックのリクエストを含むプロトコルデータ単位(unit)148(後にさらに詳細に説明する)を送信する。信用されるモジュール120は、信用されるモジュール120の外側に漏らしてはいけない信用されるモジュール120の内部の長期的な鍵を使用して、認証及び完全性チェックを行ない、追加の通信経路122cを使用して、ネットワークインターフェースカード106の赤ゾーン114に、「OK」のしるしを含むプロトコルデータ単位150を送信する。次いで、ネットワークインターフェースカード106は、通常の通信経路110を使用して、信用されるモジュール120に、何らかのデータ及び暗号解読のためのリクエストを含むプロトコルデータ単位152を送信する。信用されるモジュール120は、信用されるモジュール120内の一時的又は長期的な鍵のいずれかを使用して、データを暗号解読し、追加の通信経路122aを使用して、暗号解読されたデータを含むプロトコルデータ単位154をCPU102に送信する。そして、CPUは、適切な動作を行なう。

### 【0094】

図11は、CPU102が信用されるモジュール120からポリシー判断をリクエストするプロセスを示す。このことは、例えば、ポリシーが所定のデータを操作できるか又はアプリケーションを実行できるかどうかを、CPU102が判定しなければならないときに使用することができる。このことは、図14～図20に関連してさらに後に説明する。CPU102は、通常の通信経路110を使用して、信用されるモジュール120にリクエストを含むプロトコルデータ単位156を送信する。信用されるモジュール120は、信用されるモジュール12

0内に記憶されたポリシーにしたがって、リクエスト156を処理する。信用されるモジュール120は、認証が信用されるモジュール120から到来したことをCPU102が確信できるために、追加の通信経路122aを使用して、CPU102にレスポンスを含むプロトコルデータ単位158を送信する。動作が認証された場合、CPU102は、必要な動作を行なう。そうでなければ、プロセスを放棄する。

#### 【0095】

図12は、モジュール102、104、106の間の保護された通信を介したポリシーの制御の例を示す。この例におけるすべての通信は、追加の通信経路122を使用する。ネットワークインターフェースカード106の赤ゾーン114は、ハードディスクドライブ104行きであるプロトコルデータ単位160を、追加のデータ経路122cで信用されるモジュール120に送信する。ポリシーがこのことを許さない場合、信用されるモジュール120は、追加のデータ経路122cでネットワークインターフェースカード106に、否定を含むプロトコルデータ単位162を送信することによって、リクエストを拒絶する。後に、CPU102は、ハードディスクドライブにアドレス指定されるが追加のデータ経路122cで信用されるモジュール120に送られたプロトコルデータ単位164を送信することによって、ハードディスクドライブ104からの影響されやすいデータをリクエストする。信用されるモジュール120は、ポリシーがこのことを許すことをチェックする。これが行なわれた場合、信用されるモジュール120は、追加のデータ経路122bでハードディスクドライブ104にプロトコルデータ単位164をリレーする。ハードディスクドライブ104は、データを提供し、これをプロトコルデータ単位166内において、追加のデータ経路122bで、CPU102にアドレス指定された信用されるモジュール120に返送する。信用されるモジュール120は、ポリシーがこのことを許すことをチェックし、これが行なわれた場合、追加のデータ経路122aでCPU102にプロトコルデータ単位166をリレーする。

#### 【0096】

図13は、データが追加の通信経路122を介して渡されるデータプロトコル

単位178のフォーマットを示す。データプロトコル単位178は、次のものを有する：

- ・プロトコルデータ単位のタイプを示す識別子フィールド168
- ・プロトコルデータ単位の長さを示す長さフィールド170
- ・プロトコルデータ単位の供給源を示すソースフィールド172
- ・プロトコルデータ単位の行き先を示すデスティネーションフィールド174
- ・その他、多くの場合にデータフィールド176を含む。

#### 【0097】

すべてのフィールドが常に必要というわけではない。例えば、信用されるモジュール120のポリシーが、信用されるモジュール120内に源を発しない鍵プロトコルデータ単位のリレーを禁止するものと仮定した場合、それ故にCPU102、ハードディスクドライブ104及びネットワークインターフェースカード106は、鍵が常に信用されるモジュール120からのものであることを仮定することができる。従って、ソース及びデスティネーションフィールドは、鍵プロトコルデータ単位内に不要であり、このようなプロトコルデータ単位は、暗黙的に認証される。プロトコルデータ単位的设计及び構成及びそれ自体の使用は、通信の分野の当事者によく知られている。

#### 【0098】

今度は、前述のような信用されるコンピューティングプラットフォーム及び携帯型の信用されるモジュール（一般にスマートカード）を採用するシステムに使用するために、本発明の特定の実施形態を説明する。図14は、目的のために信用されるコンピューティングプラットフォームの特に適切な形態を示しており、プラットフォームは、図15及び図7～図13に関連して前述したシステムの発展である。図14において、ディスプレイ121は、前述のような追加の通信経路のうちの1つ122dにより信用されるモジュール120に接続される。このことは、オペレーティングシステムを含む通常のソフトウェアからの破壊の恐れなく、信用されるモジュール120をディスプレイに確実に書き込むことを可能にする。また、ホストコンピュータ100は、ビルトインスマートカードリーダー103を有するキーボード101にも接続されており、これらは、両方とも通常の通信



経路110に接続される。スマートカードリーダ103へ挿入されたスマートカードは、追加の信用されるモジュールであると考えることができ、従って信用されるモジュール120と安全に通信することができる。

#### 【0099】

本発明によれば、データに対するアクセス制限のためのシステムが構成され得るいくつかの段階が存在し、これらの段階は、一方から他方への進行と考えることができる。第1の段階は、データに加えられる操作についてのチェック及び無許可の変更に対するチェックを行ない、かつ完全性チェックによるバイパスに対して保護された、一般的な操作保護ソフトウェアを使用することである。このような操作保護ソフトウェアは、信用されるモジュール自体内で走る必要はない。好適な段階は、操作保護ソフトウェアが信用されるモジュール内で走るこのようなシステムの論理的な拡張である。何らかのデータに操作を実行するためのリクエストは、好適にはアクセスプロファイルから信用されるモジュールに送信される。信用されるモジュールにおける操作保護ソフトウェアは、このようなリクエストを評価し、アクセスプロファイル内に定義された制限に基づいて、このことを許すかどうかを決定する。好適には、信用されるモジュール及びプラットフォームのオペレーティングシステムは、これらの間の専用通信経路を有し、この通信経路は、コンピュータプラットフォームの他の部分（図14の構造におけるように）にアクセス不可能である。好適なモデルにおいて、データにアクセスするためにセキュアオペレータからオペレーティングシステムへのリクエストは、好適には専用通信経路を介して供給される。

#### 【0100】

本発明による動作に適したアーキテクチャを今説明した。次に、このようなアーキテクチャにおける本発明の実施形態を実施するための方法を以下に説明する。特定のこれらの方法は、「Computer Platforms and Their Method of Operation」と題する、本出願と同一日付の本出願人の同時係属国際特許出願に記載されたライセンスチェックのための方法と類似であるか、又はこれと共通の特徴を有し、この同時係属国際特許出願は、1999年8月13日に提出された欧州特許出願第99306415.3の優先権を主張している。

## 【0101】

システムが動作する手続きは、開発者、顧客のコンピューティングプラットフォーム（信用されるコンポーネント又はTCを保持する）及びスマートカードのような信用される携帯型のモジュール（これ以降、TPMと称する）の間において有効な特定の信用される関係におおいに依存する。もっとも一般的な場合、TCは、データがTCに（又は同様にデータがTPMに送信されるべきである場合、TPMに）送信することができるようにするために、データプロバイダで記録されなければならない。TPMも、TPMのユーザIDが、TCに発行される前に、ライセンス内に組み込むことができるようにするために、ライセンスプロバイダ（おそらくデータプロバイダと同じエンティティ）で記録されなければならない。このことは、例えば事務所の環境においてPCを任意のユーザが共有する場合のような環境に適したモデルである。しかしながら、空港のような公共の場所において機械が使用可能である場合のように、顧客の機械のユーザがあらかじめ知られていない状況において、このアプローチは不可能である。その代わりに、新しいTPMをライセンスプロバイダが発行することによって、又はこの情報がエンドユーザによってすでに保持されたものにダウンロードされるかのいずれかによって、ライセンスは、TPMのユーザIDにカスタマイズされ、エンドユーザに与えられる必要がある。ライセンスは、適宜、ソフトウェアの名称及びバージョンに対する参照、及びエンドユーザによってソフトウェアが使用され得る方法を含む。データがこのような公衆の共有の信用される端末へインストールされる場合、必要に応じて異なったアクセスプロファイルがインストールでき、このアクセスプロファイルは、ここにインストールされたデータに対してデフォルト制限、又はオーバーライディング制限、又は両方の組合せを指定することができる。例えば、文書のコピーは、特にエンドユーザがその個人のライセンス（そのTPM上に保持される）にこの許諾を持たないかぎり、禁止することができる。アクセスプロファイルが転送された（好適には暗号化されて）後、好適には完全性のチェックが行なわれ、プロファイルの要約が、ローカルTC内に記憶される。

## 【0102】

図16は、TC1103のコンポーネントの論理線図を示す。これらは、信用

されるコンポーネント1103内に、操作保護ソフトウェアコンポーネント1211及び他の操作保護データコンポーネント1210を含む。本発明の以下のコンポーネントは、前述のように保護された環境内において、及び好適にはTC1103自体内において（当業者は、適切な保護された環境がTC1103の外側に設けられ得ることを認識するとはいえ）走るべき操作保護コード1211、すなわちセキュアオペレータ1206及びデータプロテクタ1207である。TCに記憶された操作保護データコンポーネントは、信用されるエンティティによってサインされたTCの秘密鍵1201、信用されるエンティティの公開鍵証明1202、開発者の公開鍵証明1203、ログ1204、及びセキュアオペレータ1206及びデータプロテクタ1207のハッシュバージョン1205である。これらの論理コンポーネントの動作は、さらに後述する。

#### 【0103】

信用されるプラットフォーム上にデータをインストールするべきときはいつでも、完全性及び他のチェックが、第三者からデータを安全にダウンロードし又はアップグレードするために実施される。データのインストールは、このような予想された完全性の値が一致した場合に、オペレーティングシステム（「OS」）を介してのみ進行する。このようなチェックが成功した場合（データ又はラップが変更されていないという意味において）、データプロテクタは、TC（例えばスマートカード）内に、記憶されたデータに対する参照と共にデータ自体に添付されたデータ（及び任意のアクセスプロファイル）の要約を記憶する。必要に応じて、データの完全性のチェックサムのような完全性のチェックに使用される代替のデータ形態は、代わりとしてTC（例えばスマートカード）に記憶される。

#### 【0104】

図17は、顧客のコンピュータ内における保護されるソフトウェア又はデータ1306の構造を示す。顧客のコンピュータ上のデジタルデータ1304は、アクセスプロファイル1303に関連しており、このアクセスプロファイル1303内にTCの公開鍵1302が記憶されている。このデータ構造1301は、データ構造1301のハッシュバージョン1305と共に記憶されている。このハッシュバージョン1305は、クリアリングハウス又は開発者の秘密鍵でサイ

ンされる。好適には、ハッシュバージョン1305は、TC自体内に記憶される（これはインストールプロセスの間にデータプロテクタ1207によって行なわれる）。

#### 【0105】

図18は、顧客のプラットフォーム上へソフトウェア又は他のデータをロードし又はアップグレードするためのフローチャートを示す。図18に示されたステップは、データプロテクタ1207がTC1103内で走らなくてもよい一般的な場合に適用されるが、データプロテクタがTC1103内で走っている（さらに簡単な）場合に容易に適応することができる。

#### 【0106】

インストールすべきデータは、送信側の秘密鍵によってハッシュされてサインされ、これは、送信側によってデータ自体に添付される。データを送信する前に、送信側が信用されるコンピューティングプラットフォームの完全性のチェックを要求することは（前述のように）、普通である。

#### 【0107】

信用されるコンピューティングプラットフォームのオペレーティングシステム1400が、ステップ1401において、データをインストールすることをリクエストする場合、データプロテクタ1207は、ステップ1402において、リクエストを受信し、ステップ1403において、送信側に対応する公開鍵証明を使用して、このメッセージのサインをチェックし、それにより送信側の認証をチェックする。

#### 【0108】

認証が失敗した場合（ステップ1404）、データプロテクタ1207は、オペレーティングシステムにエラーメッセージを送り（ステップ1405）、オペレーティングシステム1400は、適切なメッセージを表示させる。

#### 【0109】

認証が成功した場合（ステップ1407）、データプロテクタ1207は、TC1103内において使用可能な暗号法能力を使用することによって、メッセージのハッシュを計算し、かつこれをデータに関連するメッセージハッシュと比較

する（ステップ1408）。これは、メッセージの完全性のためにチェックする。

#### 【0110】

ハッシュが同じである場合（ステップ1409）、データプロテクタ1207は、TC内にメッセージ1304及び対応するアクセス制御データ1303のハッシュ1305をセーブし（ステップ1411）、オペレーティングシステム1400が通常のようにデータをインストールできることを示す（ステップ1410）。TCは、インストールのログを作成し、これを関連するログファイル1204に加える（ステップ1412）。

#### 【0111】

ハッシュが同じでない場合（ステップ1413）、このことは、データが変更されており、これをインストールすべきでないことを示す。データプロテクタ1207は、オペレーティングシステム1400にエラーメッセージを送り（ステップ1414）、このオペレーティングシステムは、適切なメッセージをユーザに表示する（ステップ1415）。

#### 【0112】

代替の可能性は、データが信用されるコンピューティングシステムにおける後続の実行のために、ユーザのスマートカード又は他のPTMに送られる場合である。これは、データプロテクタ1207と同様なその信用される部分コード内に含むために、図6にも示したようなスマートカードである。再びPTMの完全性チェックは、一般にデータのインストールの前に必要であり、スマートカードは、データを記憶するためだけでなく、好適にはその信用される部分内にデータの要約及びアクセス制御データも記憶するための容量を必要とする。データのインストールは、そうでなければ本質的に図18に示したようなものでよい。このような装置において、動作ログ1204に対する均等物がPTM上に、好適には信用される部分内に保持されることが望ましい。

#### 【0113】

図19は、制限されるコードの実行のために本発明の実施形態に関連するPTM1106とTC1103との間の関係を示す。サインオンにおける相互の認証

が存在し、TCは、PTMのIDをチェックする（好適にはSCの公開鍵の証明を介して）、これは、図7に示したようなものであってもよい。そして、ユーザは、制限されるデータにアクセスすることを求める。TC上のセキュアオペレータ1206が、このデータにアクセスするために信用されるコンピューティングプラットフォームのオペレーティングシステム1400に対して許諾を拒絶する前に、TCは、PTM上の関連するユーザライセンスに対するチェックを行なう。従って、オペレーティングシステム1400は、データに対して信用される入力／出力プロセスを有しており、すなわち、当業者は、このことがいくつかの方法で達成できることを認識するであろうが、これらの方法のうちの特に有利な1つは、セキュアオペレータソフトウェア1206と別のソフトウェアにアクセスできないオペレーティングシステム1400との間のセキュアハードウェア通信経路であり、これは、図14のシステム内に存在する通信経路によって達成することができる。オペレーティングシステムの関連する部分は、BIS上でチェックされ、すなわち、必要に応じてシステム完全性のチェックは、オペレーティングシステムのこの部分における完全性のチェックが失敗した場合、失敗に至る。制限されたデータのユーザアクセスに対する典型的なアプローチは、以下のようになっている。ユーザが多分別のプログラムを介して特定のデータへのアクセスを望む場合、セキュアオペレータ1206は、データに関連するアクセスプロファイルを使用する（アクセスプロファイルを使用するための代替物は、最後のサインオンの間に取得されるユーザIDによって、要求された許諾を実行することを許諾が可能にするかどうか、又はさもなければこのようにするための一般的な許諾が存在するかどうか（無関係又は同一）を確認するために、任意のライセンスに関するローカルに記憶された情報の使用を採用することができる）。好適には、データプロテクタ1206も、プロファイルの及びデータの完全性をチェックする。PTMユーザIDに対して有効な許諾が見つけれられた（又は一般的な許諾が存在する）場合、許諾は、データにアクセスするためにオペレーティングシステム1400に与えられる。そうでない場合、セキュアオペレータは、質問のデータに関するライセンスがPTM1106に記憶されているかどうかを見出すために、PTM1106に質問する。そうでない場合、許諾は、操作を実施

するためのオペレーティングシステムに対して否定される。しかしながら、ライセンスがPTM1106自体上に記憶されている場合、使用許諾情報は、共有セッション鍵及びチェックされた（及びおそらく記憶された）完全性を介して暗号化されていることによって検索される。PTM1106上にライセンスが存在する場合でさえ、チェックは、現在の操作が有効であるかどうかを確認するために行なわれる必要があることがある。そうである場合、許諾は、データにアクセスするためにオペレーティングシステムに与えられ、そうでない場合、許諾は否定される。好適には、操作が行なわれる前に、TCも、そのユーザIDに対応するPTMが依然としてスマートカードリーダ内に挿入されていることをチェックする。

#### 【0114】

アクセスプロファイル及びデータが変更された場合、何に対応するエントリーであるかがはっきりしないかもしれないように、TC内に記憶された要約に対してデータが一致することができないかもしれない。従って、やはり好適には、データプロテクタは、その中に記憶された対応する適切な要約が存在しない場合、どのデータも実行することを可能にしない。

#### 【0115】

今度は、これらの原理にしたがった操作制限に対する特定のアプローチを説明する。

#### 【0116】

図20は、チェックのモデルを使用した操作制限に対するフローチャートを示しており、この場合、オペレーティングシステム1400は、TC1103内にあるセキュアオペレータ1206と、及びそのデータに関して開発者によって許された操作を指定するデータの一部に関連するアクセスプロファイル（TCの外側）と通信する。このことは、好適であるように、すべての操作保護ソフトウェアがTC1103内に搭載されている場合に適切である。オペレーティングシステム1400、操作保護ソフトウェア1211及びTC1103の間の通信は、修正又はスプーフィングに対して保護されている必要がある。前述のように、1つのオプションは、信用されるオペレーティングシステムの一部（データ入力及

び出力を取り扱う部分)を作成することにより、OSのこの部分は、BIS手続きの一部としてチェックされる完全性とすることができる。この部分が修正されている場合、プラットフォームの完全性は失われる。別のオプションは、オペレーティングシステムと通信するときに、TCからCPUに信用される通信経路(図14に示されたような)を使用することである。

#### 【0117】

このアプローチは、個々のユーザがそれぞれユーザ自身の独自のPTMを有する場合に有効である。しかしながら、これは、スマートカード又は他の適切なPTMがグループのメンバの間で複製され又は共有される場合に使用されることもできる。

#### 【0118】

オペレーティングシステム1400、信用されるコンポーネント1103、携帯型の信用されるモジュール1106(ここにおいてスマートカードとして示され、SCと省略される)及びアクセスプロファイル1303の間の適切な相互作用を有する図20に示されたステップは、以下のとおりである。

#### 【0119】

スマートカードを使用したサインオンの際、TCとスマートカードとの間の相互認証が存在する(ステップ1601)。TCは、(現在の)スマートカードIDを記憶し、これは、好適にはスマートカード公開鍵の証明である。

#### 【0120】

ユーザが何らかのデジタルデータ上で操作の実施を望むとき、一般にオペレーティングシステム1400は、データプロテクタ1207にメッセージを送信し(ステップ1602)、そして、このデータプロテクタは、TC内に記憶されたデータに又はデータ及びアクセスプロファイルの発行に対応するハッシュ又はチェックサムが存在するかどうかをチェックする(ステップ1603)。

#### 【0121】

このようなハッシュ又はチェックサムが存在しない場合、データプロテクタ1207は、メッセージをオペレーティングシステム1400にリレーし、データは実行されない。



## 【0122】

このようなハッシュ又はチェックサムが存在する場合、セキュアオペレータ1206は、TC1103の秘密鍵を使用してサインされるデータ（例えば、そのタイトル）に対する参照と共に、乱数（ナンス）を送信することによってデータのその部分に対応するアクセスプロファイル1303に、チャレンジ/レスポンスを発行する（ステップ1604）。このようなチャレンジ/レスポンスのプロトコルは、この技術内においてよく理解されている（及び例えば、図5と図7に関連して前述した）。

## 【0123】

アクセスプロファイル1303は、TC1103の公開鍵を使用して、セキュアオペレータのチャレンジを確認して認証し、メッセージを戻す（ステップ1604）。認証が成功した場合、レスポンスは、ナンス及びデータに対する参照を組み込む。ナンスは、再生攻撃に対する保護を与えるために含まれる。認証が成功しなかった場合、又はこの特定の機械上でデータ操作を行なうことを望むユーザが一人もいないので、アクセスプロファイルがエラーを通知した場合、セキュアオペレータは、メッセージをオペレーティングシステムにリレーし、データは、操作されない（ステップ1606）。

## 【0124】

セキュアオペレータは、スマートカードID及びTCIDに関して、アクセスプロファイル内に含まれた情報に依存した適切な動作チェックを行なう。さらなる情報が要求されていない場合、セキュアオペレータは、オペレーティングシステムがデータアクセスを実行することを可能にする（ステップ1607）。

## 【0125】

データに関連するアクセスプロファイルが存在しない場合、セキュアオペレータは、どのようにして続けるかのモデルを要求する。これは、スマートカード上でライセンスチェックを可能にすることがある。管理者によってその中にあらかじめセットされたデフォルトモデルは、動作に取り込んでもよい（スマートカードに対するライセンスチェックの後又はその代わりのいずれか）。これは、データアクセスを簡単に否定することができ、又はさらに精巧にすることができ、例

えば管理者は、デフォルトによって削除が起こることがあるが、所定の回数より多くのコピーが起こることはないことを規定することを望んでもよい。

#### 【0126】

明示的なアクセス許諾が与えられていない場合、又はおそらくライセンスがこのタイプのデータアクセスについてチェックされることができないというフラッグをアクセスプロファイルが含む場合、セキュアオペレータは、TCの秘密鍵を使用してサインされたデータに対する参照と共に、ナンスを送信することによってスマートカードにチャレンジ/レスポンスを発行する（ステップ1608）。そして、スマートカードは、TCの公開鍵を使用して、セキュアオペレータのチャレンジを確認して認証し（ステップ1609）、メッセージを返送する（ステップ1610）。スマートカードが関連するライセンスを含む場合、このメッセージは、ナンス、データに対する参照及びユーザアクセスライセンス情報を組み込む。そして、セキュアオペレータは、データアクセス動作を実施するためにこのライセンス内の適切な許諾についてチェックする。

#### 【0127】

アクセスプロファイル内に有効な許諾が存在しない場合、セキュアオペレータは、オペレーティングシステム1400に適切にエンドユーザに通知することを要求し、データは操作されない（ステップ1611）。

#### 【0128】

スマートカードに対するライセンスチェックの結果として生じた、有効な許諾が存在する場合、セキュアオペレータは、オペレーティングシステムにデータ操作の実行を要求する（ステップ1612）。

#### 【0129】

データ操作が許された場合、TC1103は、トランザクションの計測記録を取り、これを操作ログ1204に記憶するように適合され得る。

#### 【0130】

ソフトウェアの著作権侵害に対向するため、信用されるプラットホームの外側においてデータのコピーされたバージョンの使用に対する保護を与えることによって、今日のドングル技術において使用される技術に対応するいくつかのアプリ

一チがある。第1に、データそれ自体が、暗号化されて送信でき、かつ記憶されることができ、暗号解読鍵は、アクセスプロファイル内に、又はスマートカード上に記憶されたライセンス内に記憶される。第2に、データアクセス許諾が与えられる前に及び／又はデータアクセス操作の間に、TCID又はスマートカードID、あるいはTC又はSC内に記憶された鍵についてチェックするためにソースコードが使用可能な場合、APC呼び出しが、データ内へ挿入されることができる。開発者とのライセンス契約の外側にあるように、信用されるプラットフォーム上でデータがアクセスされ得ないことを確実にすることが唯一の目的である場合、このような測定は必要ない。

### 【0131】

デジタルデータを実行するための許諾についてチェックを強制するための好適な機構において、信用されるモジュール120（今度は図14を考慮して）は、チェック許諾のために使用されるハードウェアを含み、及び／又はソフトウェアを記憶している。特に信用されるモジュール120は、アプリケーションとコンピュータプラットフォームのオペレーティングシステム（OS）との間のブリッジとして作用する。OSは、信用されるモジュール120と好適には通常の実用アプリケーション及び非OSソフトウェアにアクセス不能なコンピュータプラットフォームのCPU102との間の通信経路122を介して与えられる信用されるモジュール120からのものを除いて、好適にはアプリケーションのロード又は実行のあらゆるリクエストを無視する。ホストコンピュータ上で動作するプロセスは、以下のとおりである。第1に、通常エンドユーザによる何らかの動作に応答して、アプリケーション又は他のデータを実行するために、信用されるモジュール120における関連する動作保護コードに対する初期リクエストが存在する。信用されるモジュール120内のセキュアオペレータは、前に詳述したように、適切なライセンスチェックを実行する。このチェックの結果が、データを実行するために適している場合、セキュアオペレータは、好適には通常の実用アプリケーション及び非OSソフトウェアにアクセス不能なCPU102への通信経路122を介してこの情報をOSに伝達する。次に、OSは、アプリケーション又はデータを実行するためにホスト上でプロセスを開始する。類似のプロセスは、データイ

ンストールが適切であることを示すために、データプロテクタがOSと通信するときに実施される。

#### 【0132】

好適には信用されるモジュールは、データを使用するためにオペレーティングシステムにリクエストをログ記録するように動作することができる。データ使用の計測のセキュリティと信頼性は、信用されるモジュール内にデータ使用を確実にログ記録することによって増強される。データ操作活動のログ記録は、TCにおいて安全に行なわれて記録される。多数の異なる段階において、このことを実行するオプションが存在する。もっとも一般的なものは、セキュアオペレータによってデータが開かれ、コピーされ、プリントされ又は実行許可される段階にある。別の共通点は、データプロテクタが、インストールされるべきデータに対するその完全性のチェックを成功して完了し、及びこのデータを顧客の機械へ成功してインストールした段階にある。アクセスプロファイル、セキュアオペレータ及びデータプロテクタは、完全性のチェックによって保護されているので、ログ記録プロセスをバイパスし又は編集するハッカーの試みに対して、何らかの保護が与えられる。このようなログは、セキュア検査情報、及び融通性のある使用許諾及び支払いモデルの可能性の両方を提供する。このような検査ログは、使用報告、及び機械ユーザのIT部門または会社の検査者のような第三者にアクセス可能な情報のための基礎をなしている。

#### 【0133】

有利な点は、API呼び出しは、信用されるモジュール内における秘密の存在、信用されるモジュールのアイデンティティ及び存在、又は携帯型の信用されるモジュールに関連するユーザIDのようなデータ制限に関連する情報に対するチェックのために、信用されるモジュールに対して又は操作保護コードに対して使用することができる。さらに、信用されるモジュールは、コードの一部を実行するようにすることができる。信用されるモジュールの強力な認証は、信用されるモジュールの秘密暗号鍵および標準的な認証プロトコルを使用することによって可能である。

#### 【0134】

このようにして（繰り返して言えば、通常のドングルのためにAPI呼び出しを使用する）、API呼び出しの使用において開発者のための利益がある。ソフトウェアにAPI呼び出しを加える通常の利益は、実行可能な又はソースのコードが明確に得られる場合でさえ、ソフトウェアが特定のユーザにカスタマイズされ、ひいては別の認証されたユーザに対して、ただちに利益のあるものではない。しかしながら、従来の構成において、このことは、開発者の一部に対して多大な努力を必要とすることがある。唯一の相違が異なった信用されるモジュールIDである場合、コードの完全性チェックを介した保護によって、実質的な保護は、信用されるモジュール自体内におけるコードの実行部分が個々のコードのカスタマイズを必要としないとき、開発者によるきわめてわずかな努力によって取得できる。

#### 【0135】

この場合、開発者は、プラットフォームの信用されるモジュールにおける秘密（例えば、携帯型の信用されるモジュールにおけるユーザID）の存在に関してチェックするためのソフトウェア内にAPI呼び出しを挿入することができる。一般に、セキュアオペレータは、概して実行時にチェックをさせるだけであり、コード内におけるさらなるAPI呼び出しは、所望の場合、コードの実行の間に種々の段階において行なうことができる。このことは、ソフトウェアに対する一般的な方法で（すなわちそれぞれの顧客が同じバージョンを受信する）行なうことができ、正確な信用されるモジュールIDのようなカスタマイズされた詳細は、後に追加されることができる。

#### 【0136】

データプロテクタの役割は、データが安全にインストールされることを（図18に関連して説明したように）確実にし、データに対する関連した操作の前にデータ及び任意の関連するアクセスプロファイルの両方の完全性をチェックすることでもある。この役割に対する論理的な拡張が存在し、これは、さらなる利益を提供する。データの完全性のチェックは、ラッパが取り除かれた場合にデータが実行されることに対してさらなる保護を与えるために、データプロテクタによってラッパなしのデータが実行されることを防止できるようなものであってもよい。

。必要に応じて、チェックは、データの複数のコピーが存在しないことを確実にするために、データプロテクタによっても行なわれ、このことは、例えばユーザのセット数を含む又は所定の時間にわたって実行する使用許諾モデルによって保護されるデータの使用の認証されていない拡張を防止する。複数のコピーが見つかった場合、ユーザは、このコピーの実行を可能にするために、1つを除いたすべてのコピーを消去するオプションを与えられる。

#### 【0137】

システムの鍵コンポーネントは、データに関連するアクセスプロファイルである。これは、保護されるべきデータを指定し、ユーザがその特定のソフトウェア又はデータ上で実行することを許された操作も指定する。本発明の態様の操作において、アクセスプロファイルは、携帯型の信用されるモジュール内に保持されるユーザIDが、データ上の所定の（又は任意の）操作を可能にするためにチェックされることを指定する。アクセスプロファイルは、携帯型の信用されるモジュールがユーザライセンスについてチェックされることも可能にする（又はこれは、特定のデータに対して許されないかもしれない）。アクセスプロファイルの完全性がプラットフォームの信用されるコンポーネントによってチェックすることができる場合、アクセスプロファイルは、プラットフォームの信用されるモジュール内に、又は信用されるプラットフォームのどこか他に配置されることができる。アクセスプロファイルは、データに関連するライセンス又は暗号コンテナと同様である。

#### 【0138】

この手続きに関する変形が存在し、この場合、プロファイルがさらに事前対応型であり、オペレーティングシステム1400がデータに対する操作をリクエストするためにアクセスプロファイルに直接接触し、操作がプロファイル仕様に逆らうことがない場合にだけ、アクセスプロファイルが許諾によって応答する。同様に、スマートカードのユーザライセンスは、適切なチェックを開始することができる。

#### 【0139】

このような構成において、これは、データに対する操作に関してオペレーティ

ングシステムを制御するセキュアオペレータというよりはむしろアクセスプロファイルである。この場合、アクセスプロファイルにとって、プラットフォームの信用されるモジュール内に完全に又は部分的に（好適にはオペレーティングシステムへのセキュア通信経路と共に）配置されることは有利である。今度は、図22に関連して、コンピュータプラットフォーム上へのデータのインストール、及び携帯型の信用されるモジュールを有するユーザによるデータの後続の実行を説明する。

#### 【0140】

データに関する登録及び／又は支払いの際、ステップ2201において、クリアリングハウス又は開発者（正確な支払いモデルにしたがって）は、スマートカードID（やがて携帯型の信用されるモジュールに記憶されるべき）及び購入されたデータにしたがって更新されるべきデータに対応するライセンスを認証する。（これに先立って、相互認証（おそらくオフライン）があり、これらの本体間の公開鍵証明は交換されており、さもないと開発者は、携帯型の信用されるモジュールを含むスマートカードを実際に発行する）。クリアリングハウス又は開発者は、（カスタマイズされた）アクセスプロファイルに関連してデータを顧客に送信する（ステップ2202）。携帯型の信用されるモジュールの公開鍵が、アクセスプロファイルへ挿入される（代案として、共有の鍵が、セキュアオペレータとスマートカード携帯型の信用されるモジュールとの間にセットアップされる）ように、アクセスプロファイルは、カスタマイズされる。データ及びアクセスプロファイルの両方は、クリアリングハウス／開発者の秘密鍵によってハッシュされてサインされ、これに対応する公開鍵は、スマートカード上の携帯型の信用されるモジュール内に記憶される。保護されるべきあらゆるメッセージの内容は、ランダムに発生される秘密鍵（DES鍵のような）を使用して暗号化され、標準的なプロトコルにしたがって意図した受取側の公開鍵を使用して暗号化された公開鍵（例えば、RSA）である対称鍵と共に転送される。データがコンピュータプラットフォームに転送されると、同様なプロセスは、データの転送に対して行なわれ、開発者の公開鍵は、コンピュータプラットフォームの信用されるモジュールに送信される。

## 【0141】

データプロテクタは、データがコンピュータプラットホームに転送される時にはいつでも、データの完全性をチェックし、インストールの際（ステップ2203）、パッケージは、ハッシュ及び（プラットホームの信用されるコンポーネントにおける公開鍵を使用して）暗号解読されたサインとの比較によって確認され、ハッシュは、プラットホームの信用されるコンポーネント内に記憶される。予想されたものでないデジタルサインが、生まれた場合、データもアクセスプロファイルもロードされない。

## 【0142】

前述のステップは、データのインストールに関しており、以下のステップは、データへのアクセスを制限するためのシステムの使用に関する。スマートカードを使用してサインオンする際、プラットホームの信用されるコンポーネントとスマートカードの携帯型の信用されるモジュールとの間に相互認証が存在する（ステップ2204）。

## 【0143】

プラットホームの信用されるコンポーネントは、（現在の）スマートカードユーザIDを受信して記憶する（ステップ2205）。

## 【0144】

ユーザがデータの使用を望むとき、コンピュータプラットホームのオペレーティングシステムは、そのデータに対応するアクセスプロファイルからの動作を要求する。アクセスプロファイルは、データに対する参照と共に、乱数（ナンス）を送信することによりセキュアオペレータにチャレンジ／レスポンスを発行する（ステップ2206）。

## 【0145】

セキュアオペレータは、スマートカードIDを使用して、さもなければスマートカード上に記憶された何らかの情報を取得することによって、データに対する適切なチェックを行なう（ステップ2207）。例えば、セキュアオペレータは、プラットホームの信用されるコンポーネント内に記憶されたプロファイルにおいて、挿入されたスマートカードのユーザIDにしたがってデータが使用される



ことを許諾されているかどうかをチェックすることができ、又はプラットフォームの信用されるコンポーネント内に記憶されたプロファイルにしたがって信用されるプラットフォーム自体において（ユーザに関係なく）データが使用されることを許諾されているかどうかをチェックすることができ、又はアクセスされるべきデータに関連して内部に記憶された何らかのライセンスのさらなる詳細を取得するためにスマートカードを調べることができる。この場合、セキュアオペレータは、プラットフォームの信用されるコンポーネントの秘密鍵を使用してサインされたデータに対する参照と共に、ナンスを送信することによってスマートカードにチャレンジ/レスポンスを発行する。次に、スマートカードは、プラットフォームの信用されるコンポーネントの公開鍵を使用してセキュアオペレータのチャレンジを確認して認証し、ナンス、データに対する参照及びユーザアクセスライセンス情報を組み込んだメッセージを返送する。そして、セキュアオペレータは、データアクセス動作を実行するために、このライセンス内の適当な許諾についてチェックする。

#### 【0146】

有効なライセンスが存在しない場合、セキュアオペレータは、エラーメッセージを返送し（ステップ2208）、このエラーメッセージからアクセスプロファイルは、適切にオペレーティングシステムを使用許諾して通知することによって、問題の正確なタイプを判定することができる。有効なライセンスが存在する場合、セキュアオペレータは、コンピュータプラットフォームの信用されるコンポーネントの秘密鍵を使用してサインされて暗号化されたナンス及びデータ参照を組み込んだメッセージを返送する。

#### 【0147】

アクセスプロファイルは、コンピュータプラットフォームの信用されるコンポーネントの公開鍵を使用して、セキュアオペレータのレスポンスが適正であるかどうかを確認し（ステップ2209）、データを実行するためにオペレーティングシステムに呼び出しを渡すか、又は適宜にオペレーティングシステムにエラーメッセージを送信する。

#### 【0148】

データへのアクセスは、ログ記録される（ステップ2210）。ログは、有利にはコンピュータプラットフォームの信用されるコンポーネント内に保持されるが、追加的に又はその代わりにスマートカード内に保持されてもよく、適切に更新される。

#### 【0149】

当業者は、特許請求の範囲に記載したような本発明の範囲から逸脱することなく、前述の実施形態に多くの変形を行なうことができることを容易に認識するであろう。

#### 【図面の簡単な説明】

##### 【図1】

本発明の実施形態を実施することができるシステムを示す線図である。

##### 【図2】

スマートカードリーダーを介してスマートカードと、及びモジュールのグループと通信するために構成された信用される装置を含むマザーボードを示す線図である。

##### 【図3】

信用される装置をさらに詳細に示す線図である。

##### 【図4】

コンピューティング装置の完全性メトリックスの取得に含まれるステップを示すフロー線図である。

##### 【図5】

信用されるコンピューティングプラットフォームとその完全性を確認する信用されるプラットフォームを含むリモートプラットフォームとの間の通信の確立に含まれるステップを示すフロー線図である。

##### 【図6】

本発明の実施形態にしたがって使用するためのユーザスマートカードの使用できる部分を示す線図である。

##### 【図7】

スマートカードとホストプラットフォームを相互に認証するプロセスを示すフロ

一線図である。

【図8】

図15のシステムにおける信用されるモジュールの略ブロック図である。

【図9】

内部に使用された種々の通信方法を示すために図15のシステムの一部を示す図である。

【図10】

内部に使用された種々の通信方法を示すために図15のシステムの一部を示す図である。

【図11】

内部に使用された種々の通信方法を示すために図15のシステムの一部を示す図である。

【図12】

内部に使用された種々の通信方法を示すために図15のシステムの一部を示す図である。

【図13】

図15のシステムに使用されるプロトコルデータユニットのフォーマットを示す図である。

【図14】

本発明の特定の実施形態を説明するために使用される図15のシステムに対する修正案を示す図である。

【図15】

別の特許出願（国際特許出願第PCT/GB00/00504号、2000年2月15日出願）の主題であるホストコンピュータシステムの略ブロック図である。

【図16】

図14のシステムにおける信用されるモジュールの論理コンポーネントの線図である。

【図17】

図14のシステムにおいて保護されるソフトウェア又はデータの構造を示す図である。

【図18】

図14のシステムにおけるソフトウェア又は別のデータのインストール又はアップグレードを示すフローチャートである。

【図19】

本発明の実施形態によるシステムにおける携帯型の信用される装置と信用されるプラットフォームとの間の関係を示す線図である。

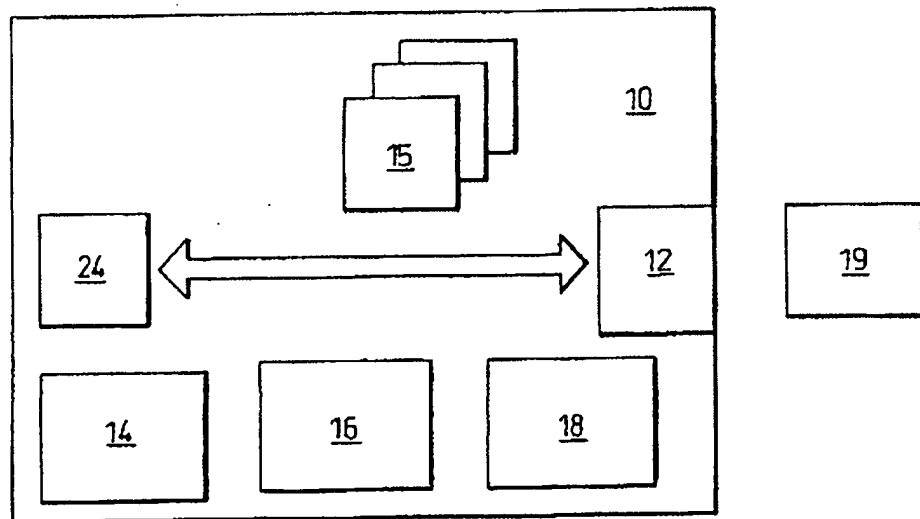
【図20】

使用許諾の制限を強制するように図14のシステムにおける保護されるデータ又はソフトウェアの使用を示すフローチャートである。

【図21】

本発明の別の実施形態において、図14のシステム上のソフトウェア又は別のデータのインストール及び使用を示すフローチャートである。

【図1】



*Fig. 1*

【図2】

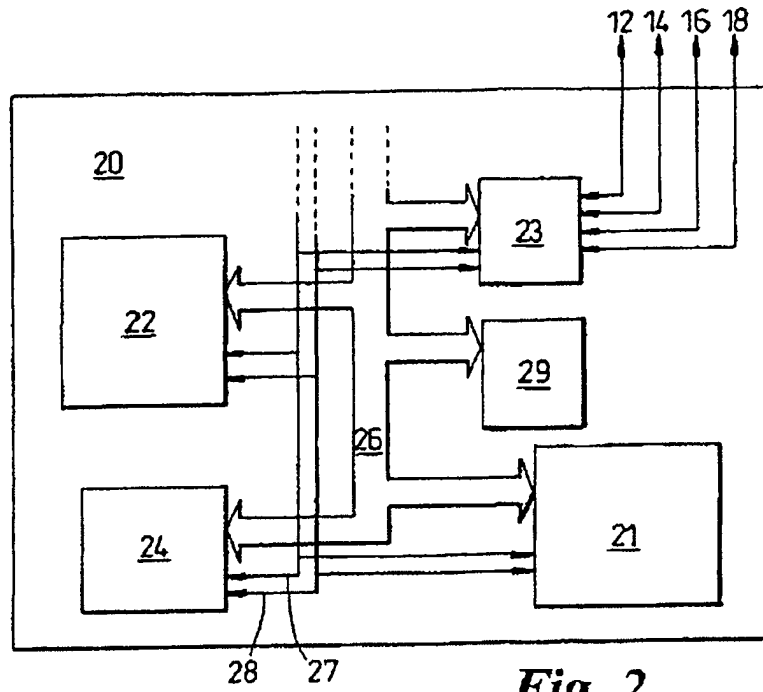


Fig. 2

【図3】

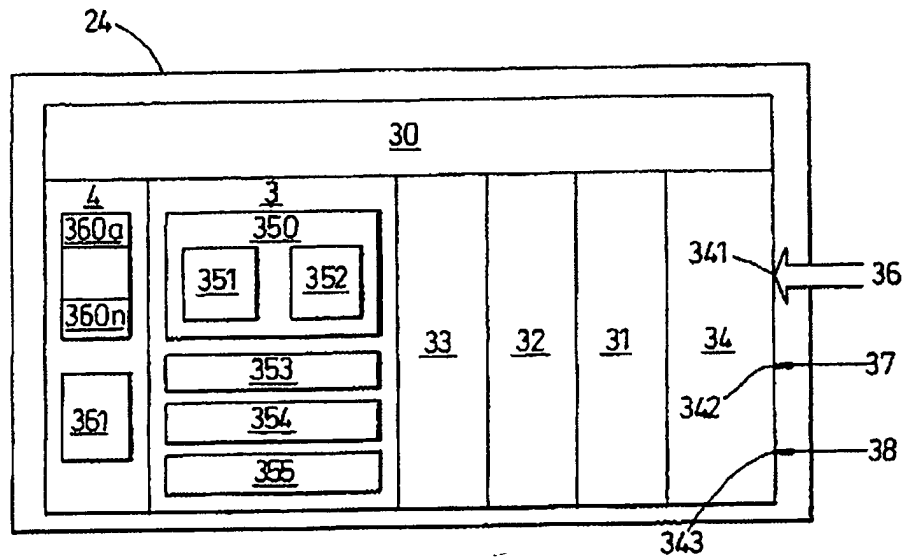
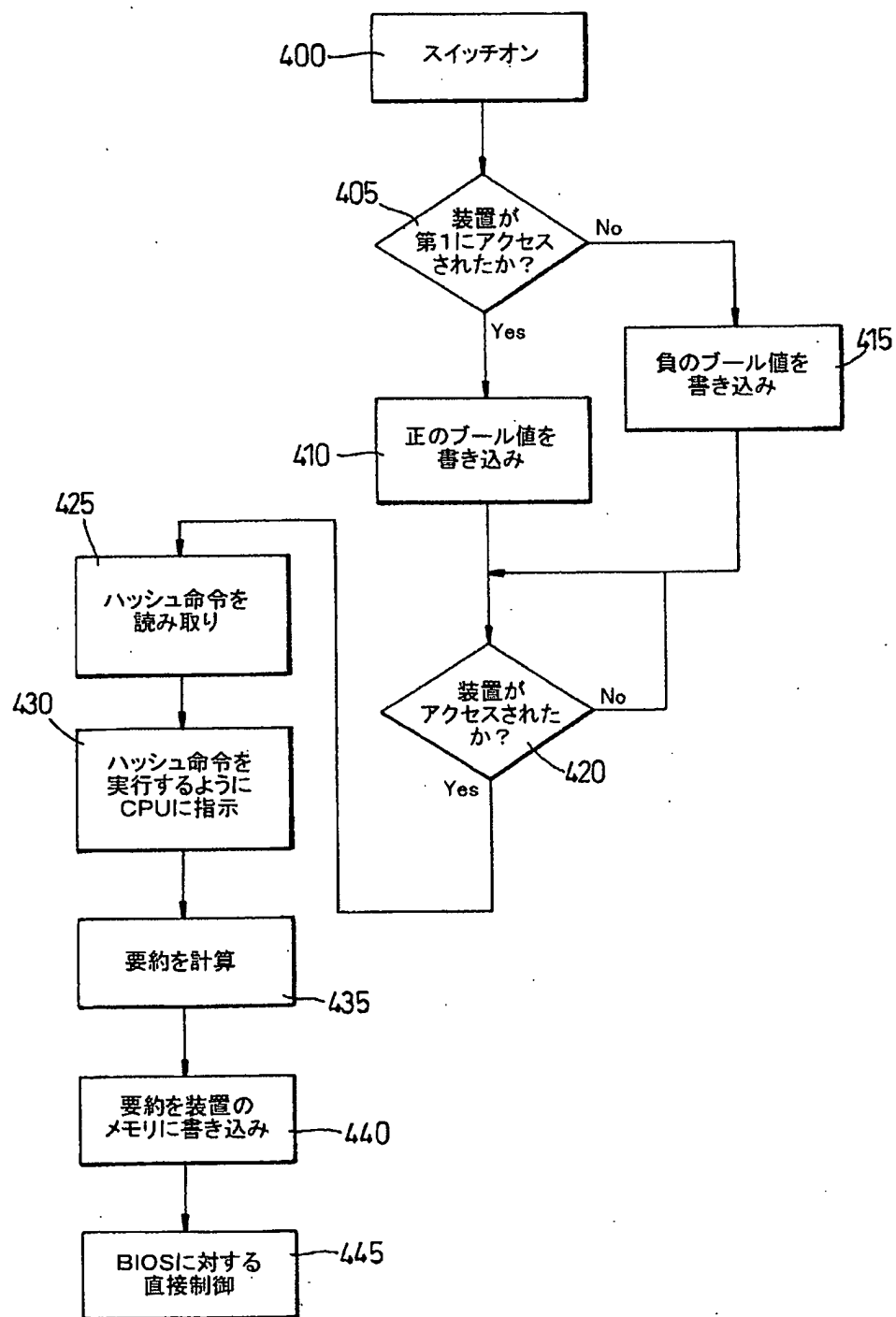
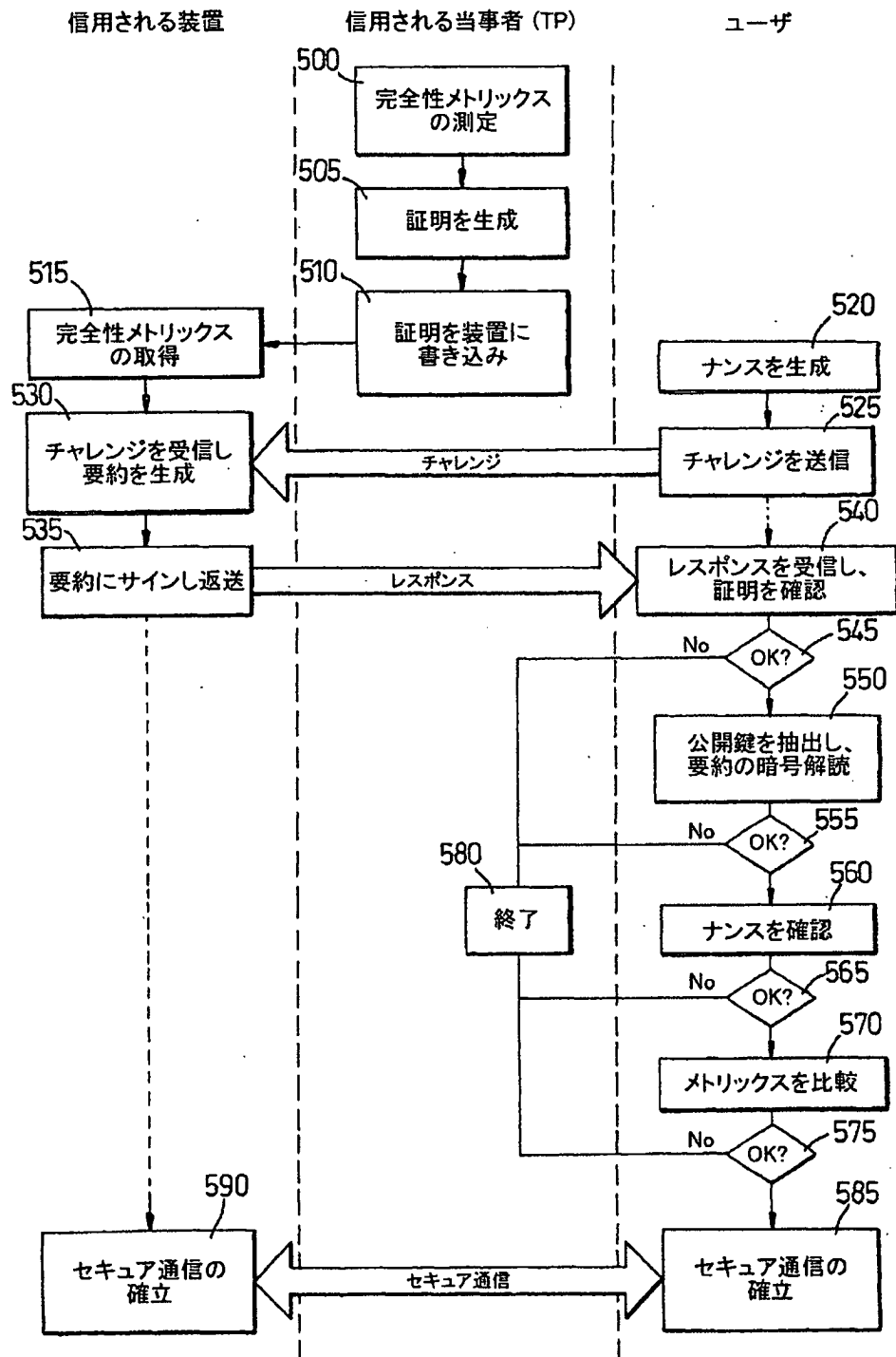


Fig. 3

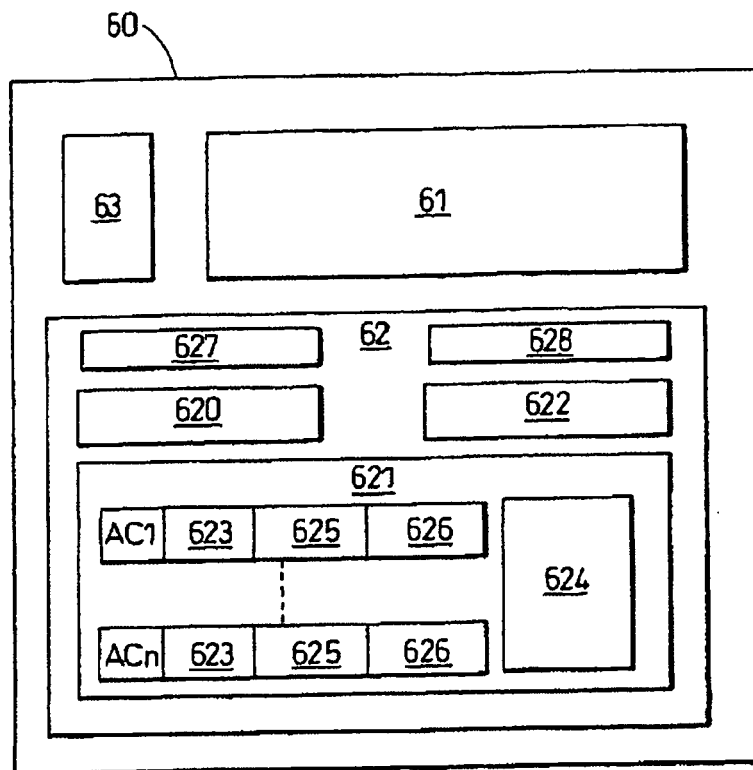
【図4】



【図5】

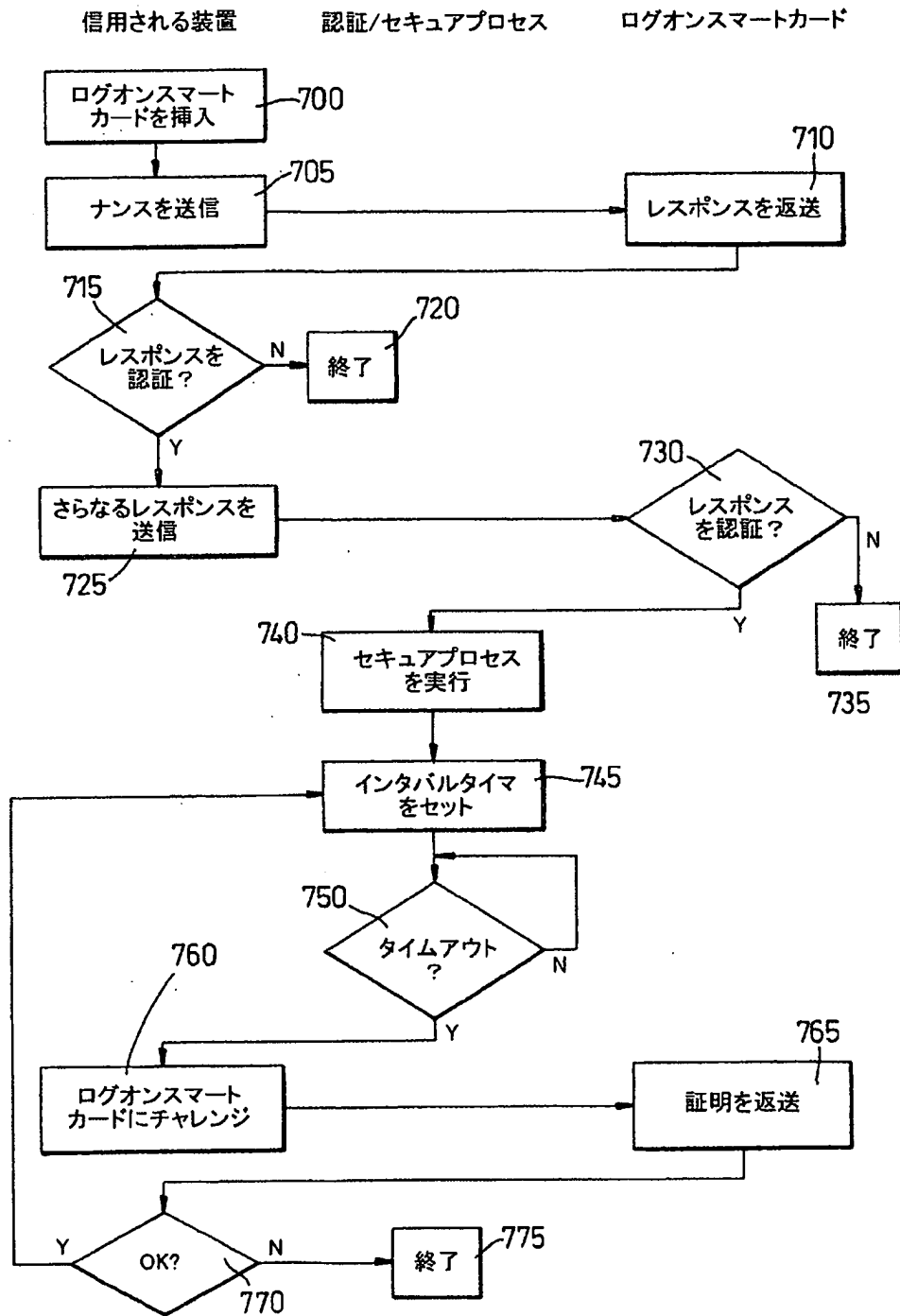


【図6】

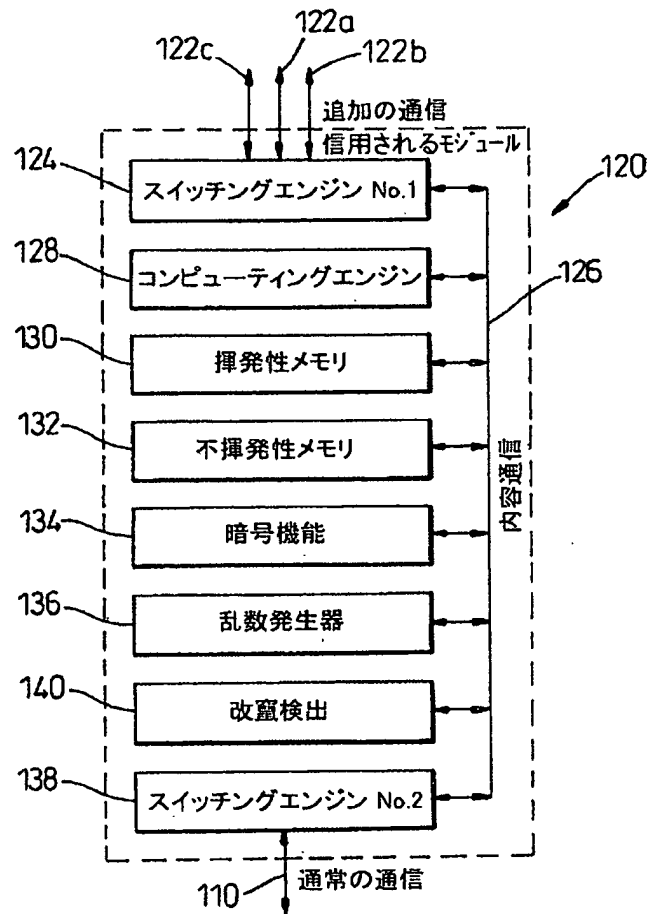
*Fig. 6*



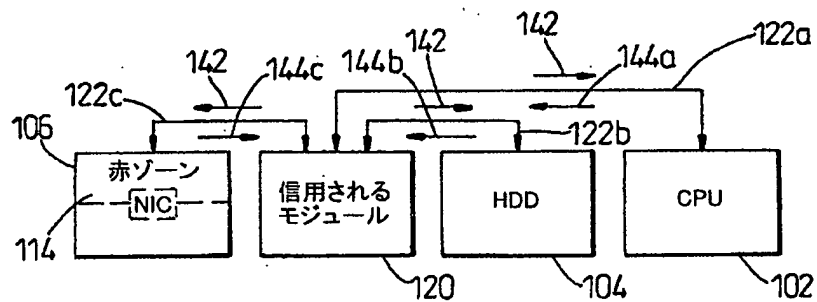
【図7】



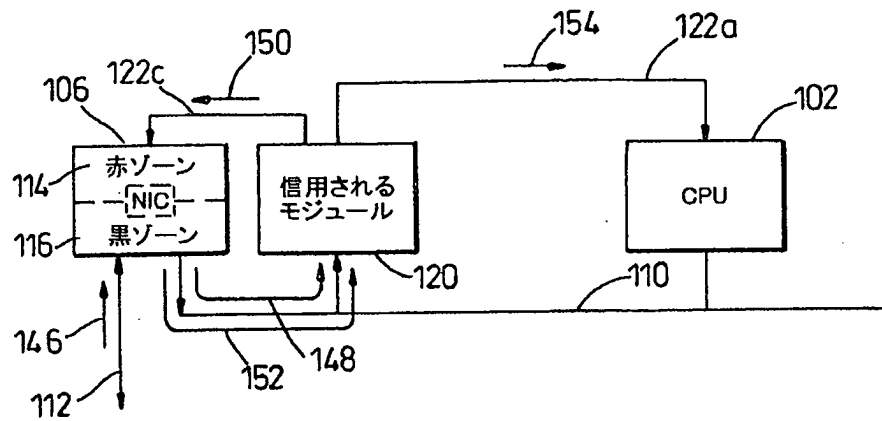
【図8】



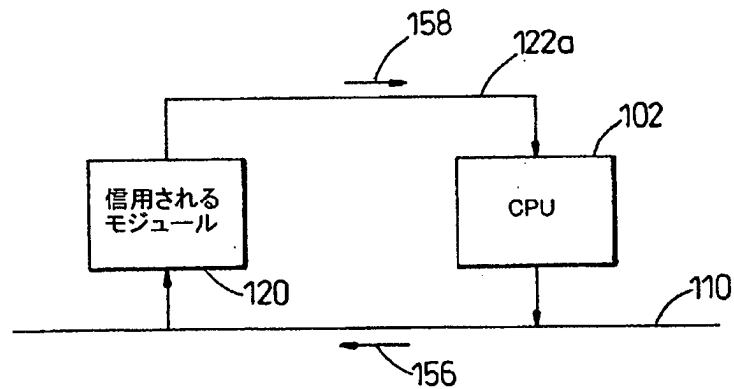
【図9】



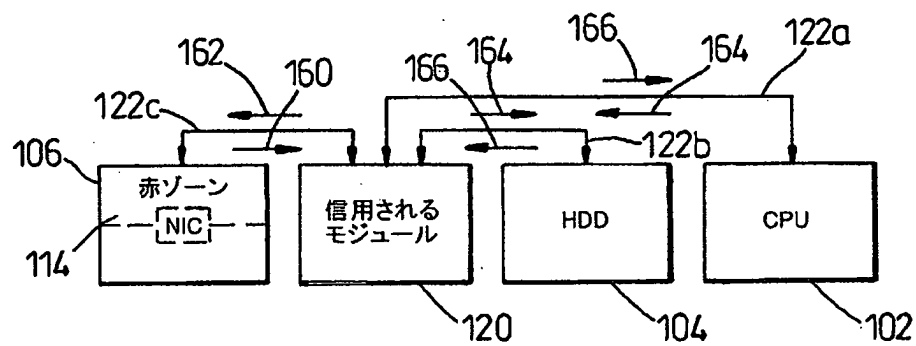
【図10】



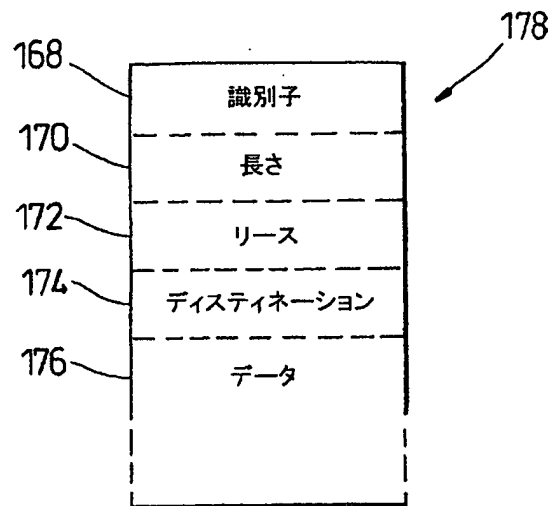
【図11】



【図12】



【図13】



【図14】

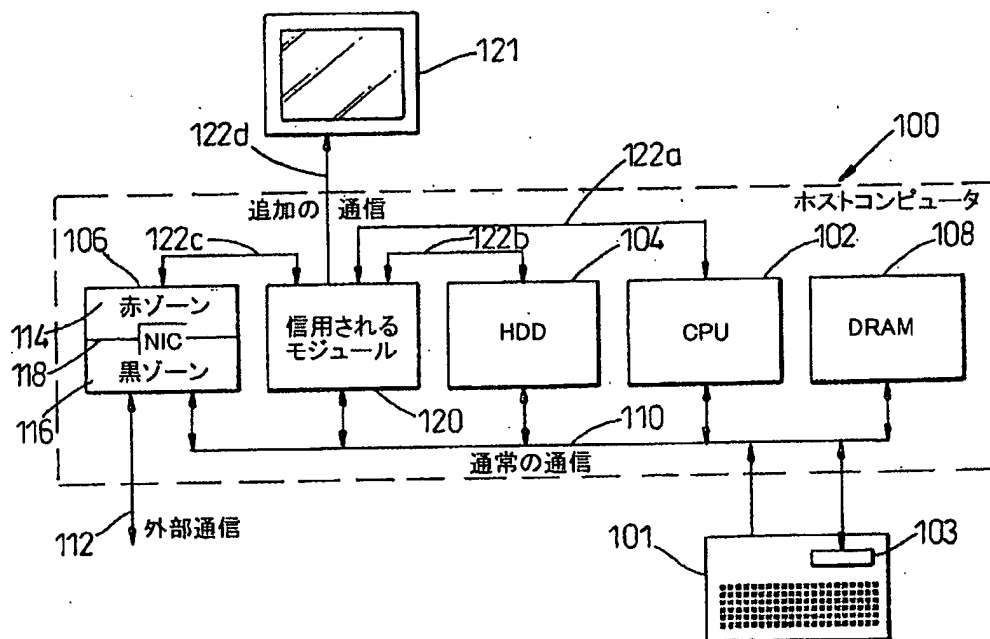


Figure 12 is a block diagram illustrating a secure system architecture. The system is organized into two main functional blocks, 1210 and 1211, which are part of a larger system 1103.

Block 1210 contains the following components:

- 1201: TCの秘密鍵 (TC Secret Key)
- 1202: 信用されるエンティティの公開鍵の証明 (Proof of Public Key of Trusted Entity)
- 1203: クリアリングハウス/開発者の公開鍵の証明 (Proof of Public Key of Clearing House/Developer)
- 1204: 動作ログ (Operation Log)
- 1205: 1202によってサインされた1206と1207のハッシュバージョン (Hash version of 1206 and 1207 signed by 1202)

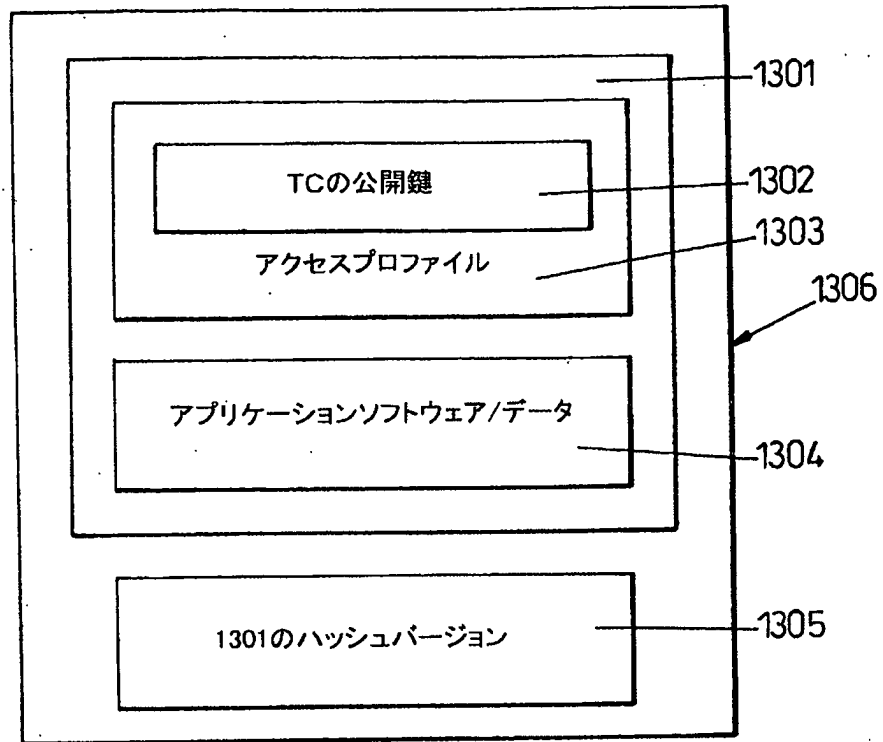
Block 1211 contains the following components:

- 1206: セキュアオペレータ (Secure Operator)
- 1207: データプロテクタ (Data Protector)

The entire system is labeled 1103.

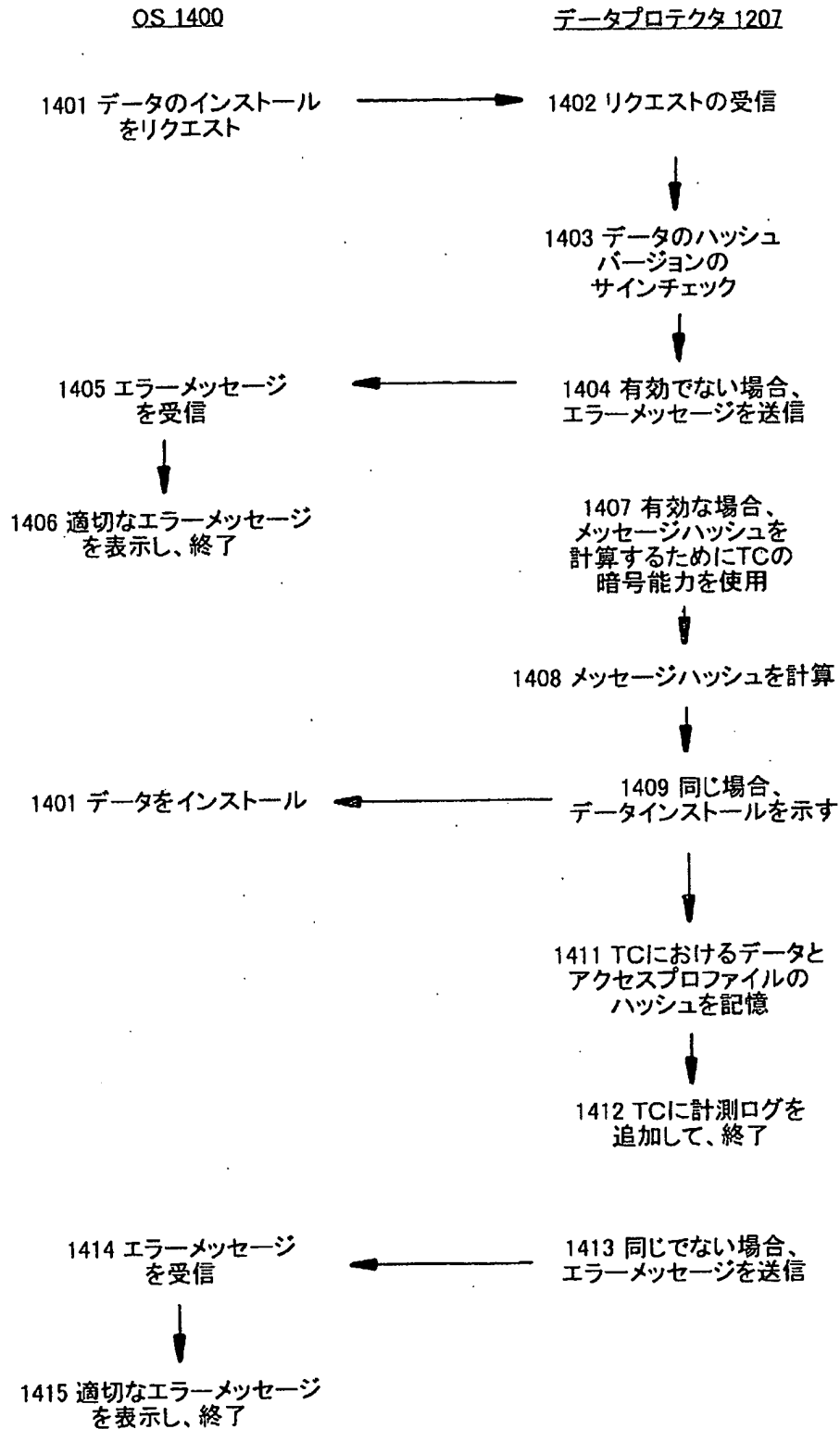
-77-

【図17】

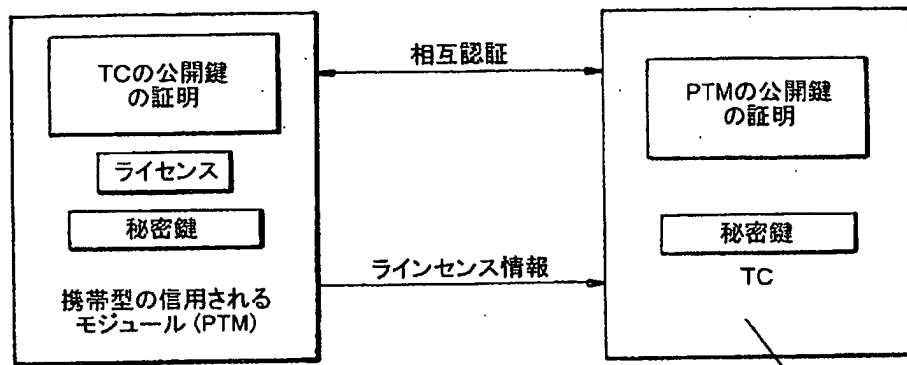


顧客のPCに搭載されたアプリケーション  
ソフトウェア/データの論理線図

【図18】



【図19】

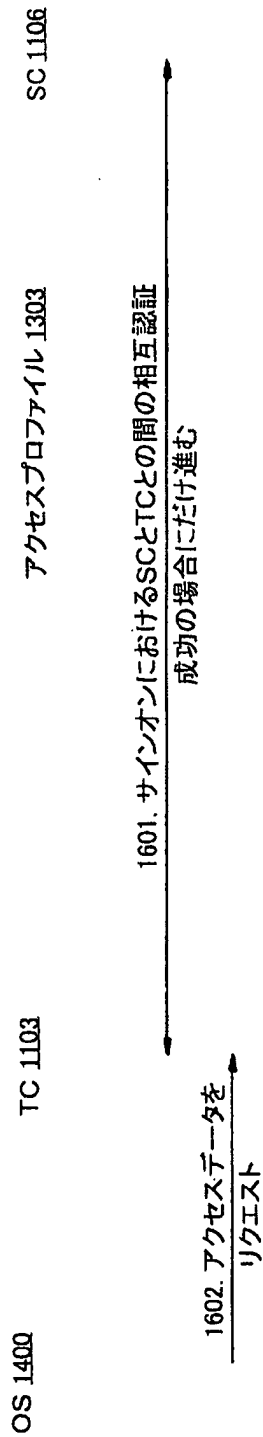


携帯型の信用されるモジュールとPCのTCとの関係

1103



【図20-1】

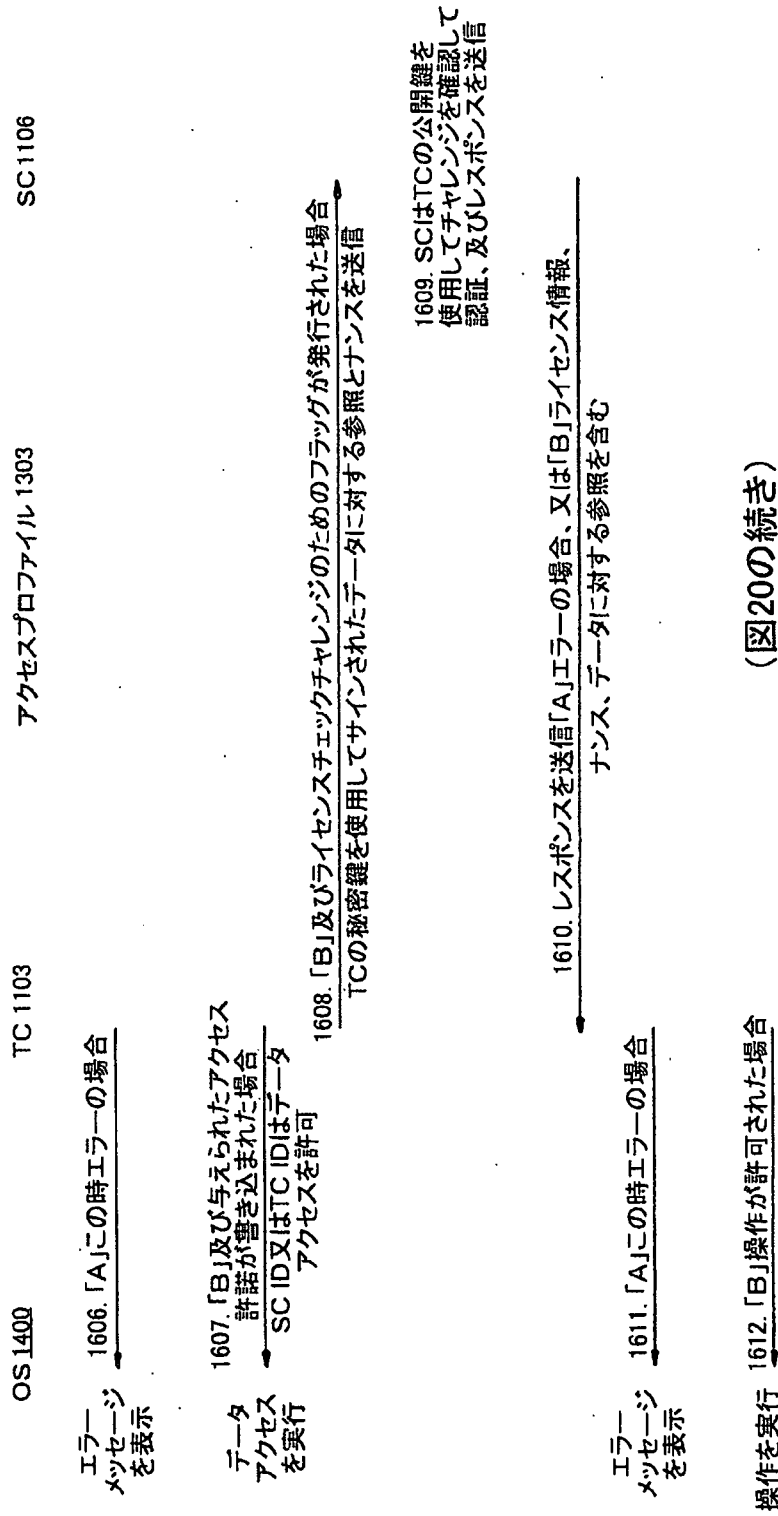


1603. データプロテクタがTCに記憶された要約と、データ及びアクセスプロファイルの完全性を照らし合わせ、成功した場合にだけ進み、そうでなければ、OSに対して許諾を否定

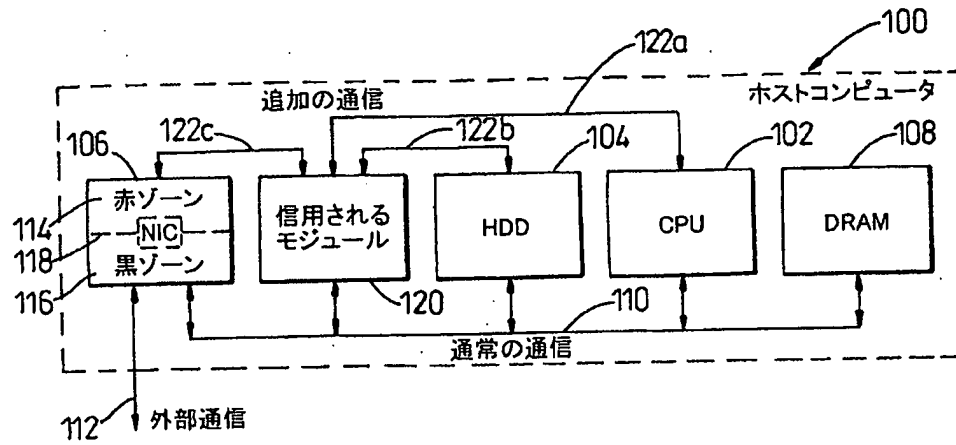
1604. TCの秘密鍵を使用してサインされたデータに対する参照、ナンスを含むチャレンジを発行

1605. TCの公開鍵によってアクセスプロファイルを確認およびチャレンジを認証、メッセージはレスポンスを送信-「A」エラーの場合、又は「B」データに対する参照、プロファイル、ナンスを含む

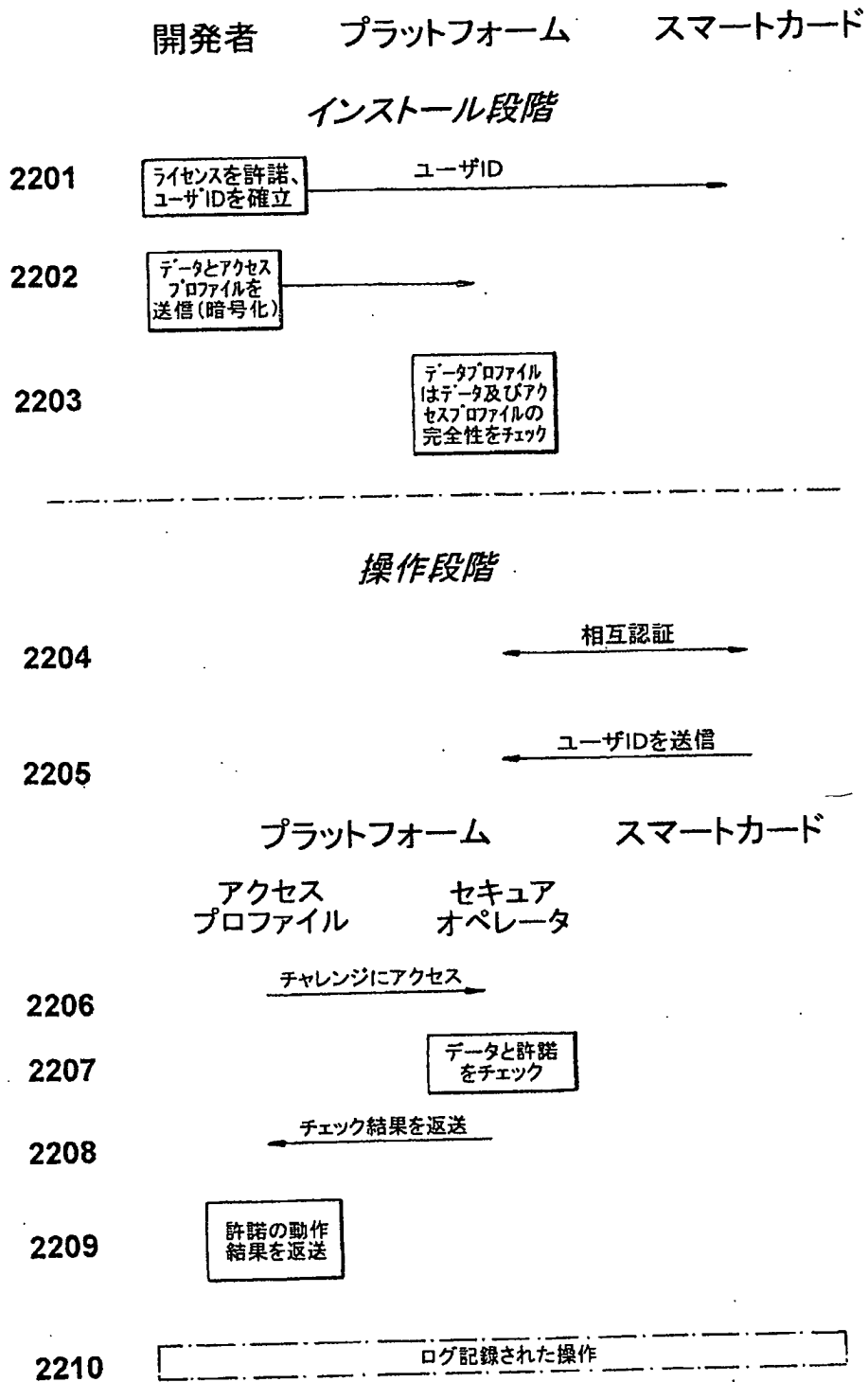
【図20-2】



【図21】



【図22】



## 【手続補正書】

【提出日】平成14年2月14日(2002. 2. 14)

## 【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】0084

【補正方法】変更

【補正の内容】

## 【0084】

今度は、図15及び図8～図13を参照して、2000年2月15日に出願された国際特許出願第PCT/GB00/00504号の主題であるシステムの特定の実施形態を説明する。このシステムは、本発明の用途に特に適している。図15において、ホストコンピュータ100は、主CPU102、ハードディスクドライブ104、PCIネットワークインターフェースカード106及びDRAMメモリ108を有し、従来の(「通常の」)通信経路110(ISA、EISA、PCI、USBのような)をそれらの間に備える。ネットワークインターフェースカード106は、ホストコンピュータ100の外側の世界との外部通信経路112も有する。

## 【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】0139

【補正方法】変更

【補正の内容】

## 【0139】

このような構成において、これは、データに対する操作に関してオペレーティングシステムを制御するセキュアオペレータというよりはむしろアクセスプロファイルである。この場合、アクセスプロファイルにとって、プラットフォームの信用されるモジュール内に完全に又は部分的に(好適にはオペレーティングシステムへのセキュア通信経路と共に)配置されることは有利である。今度は、図21に関連して、コンピュータプラットフォーム上へのデータのインストール、及び携

帯型の信用されるモジュールを有するユーザによるデータの後続の実行を説明する。

【手続補正3】

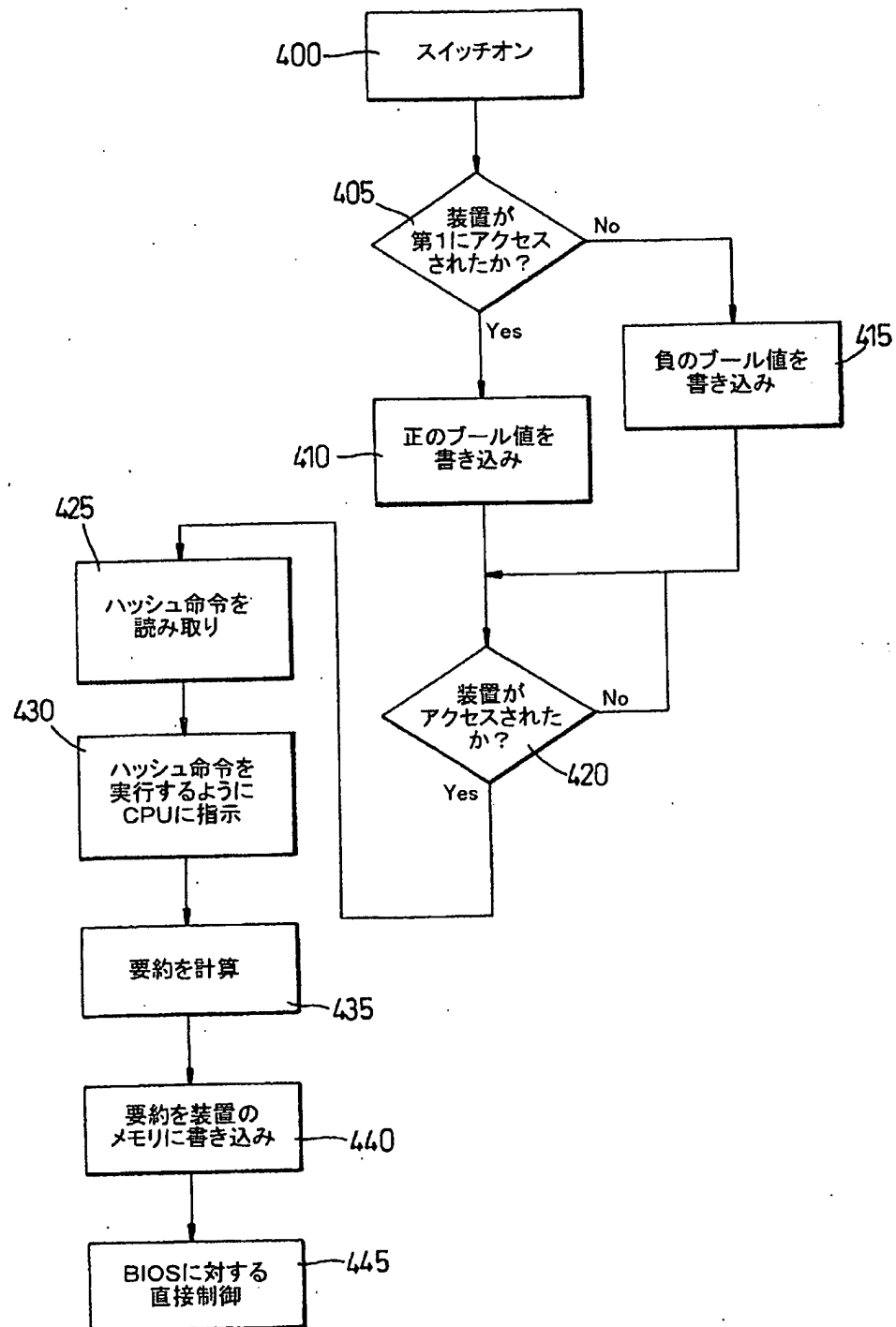
【補正対象書類名】図面

【補正対象項目名】全図

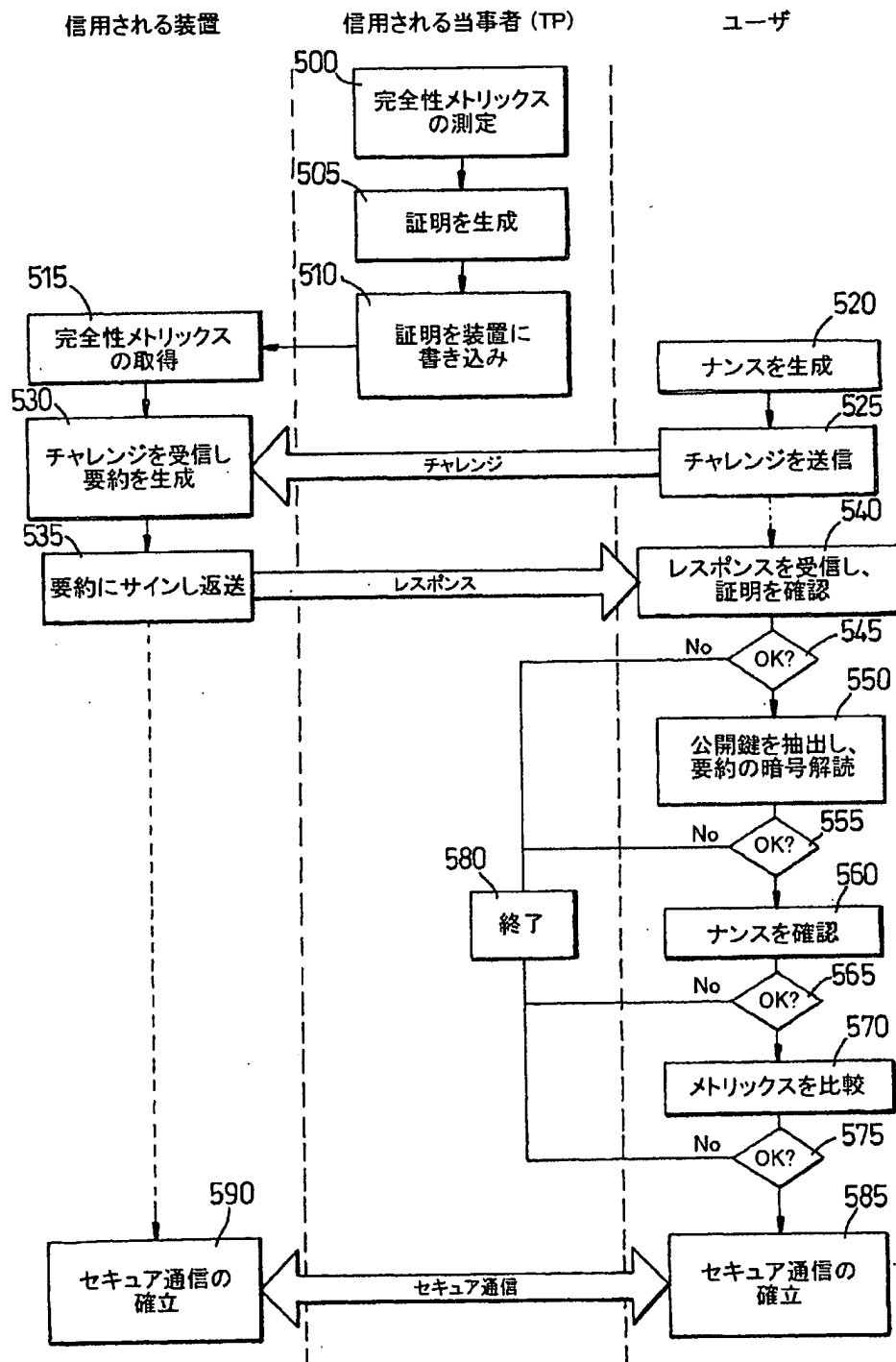
【補正方法】変更

【補正の内容】

【図4】

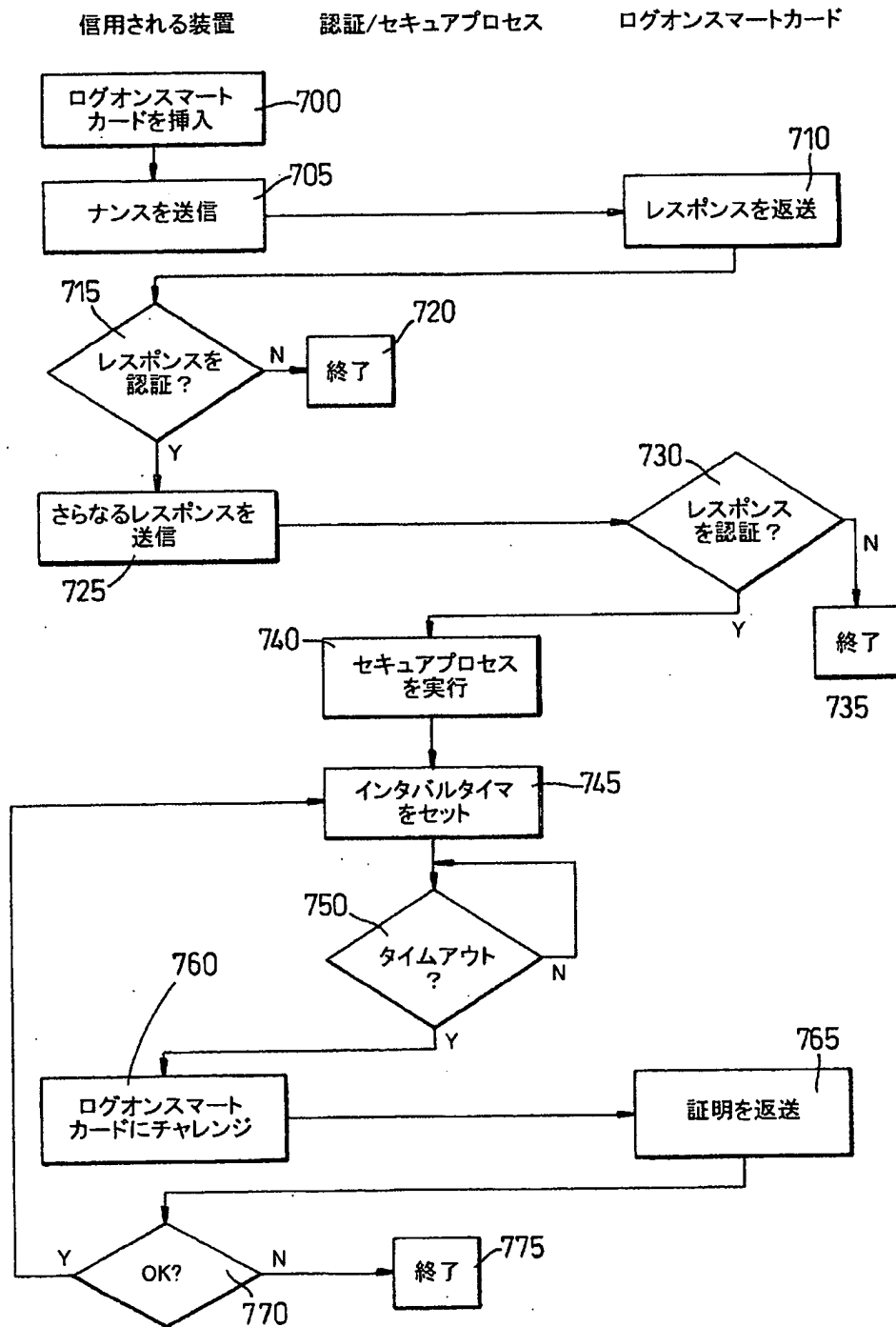


【図5】

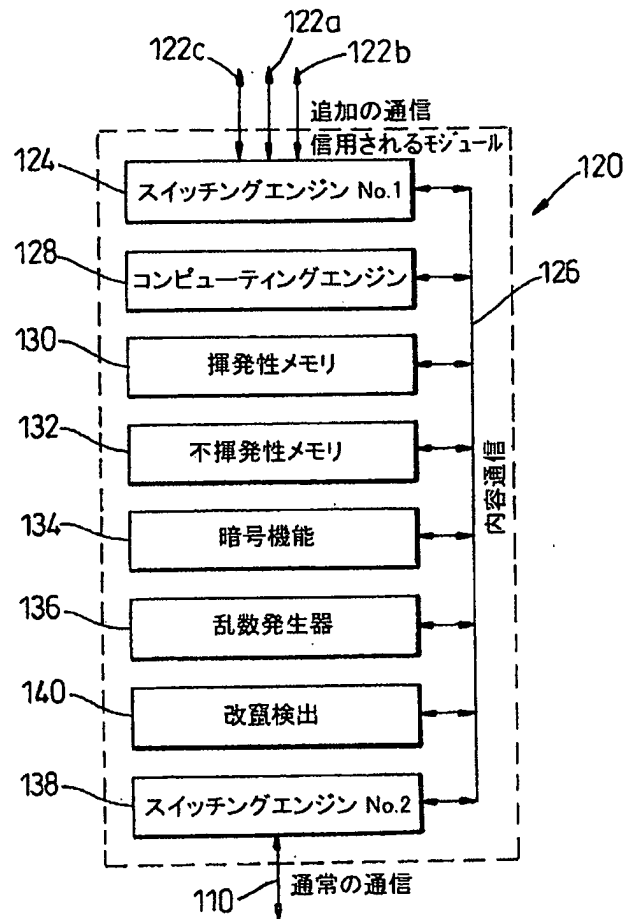




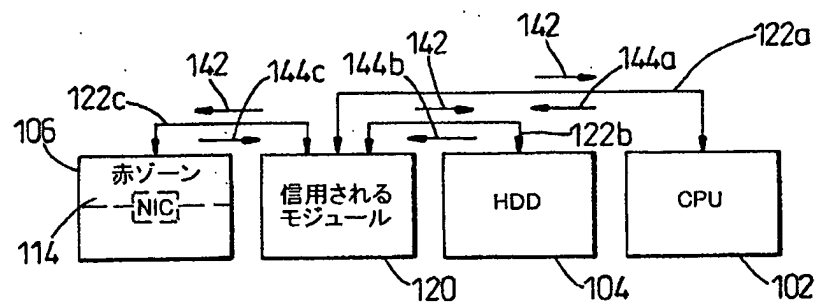
【図7】



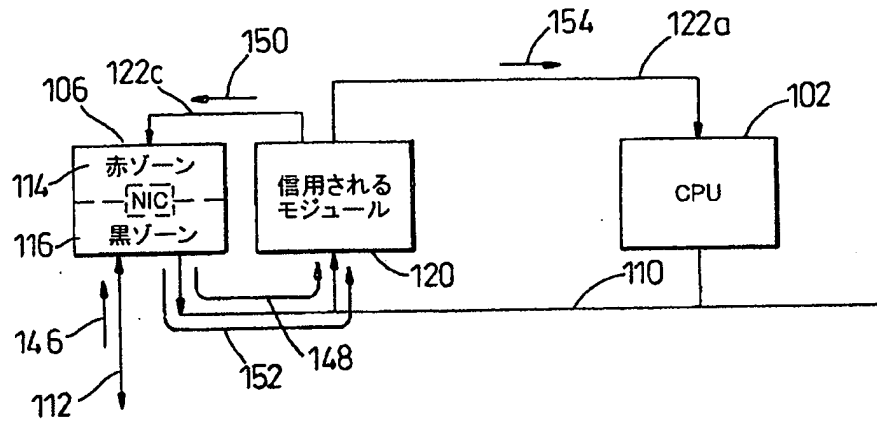
【図8】



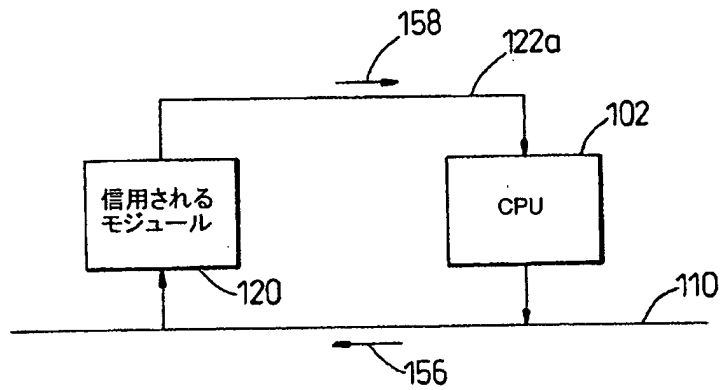
【図9】



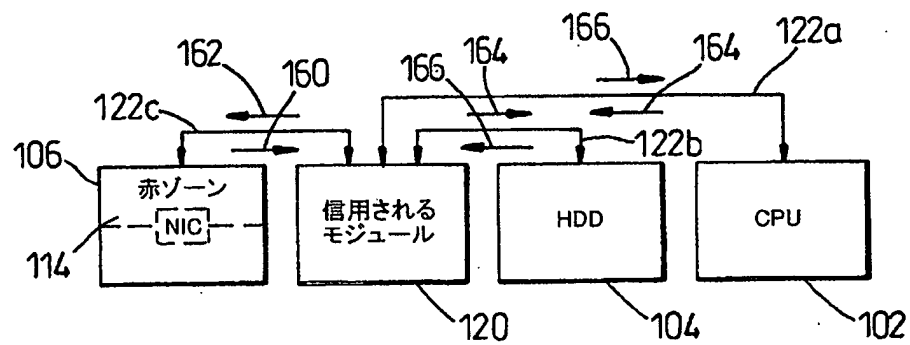
【図10】



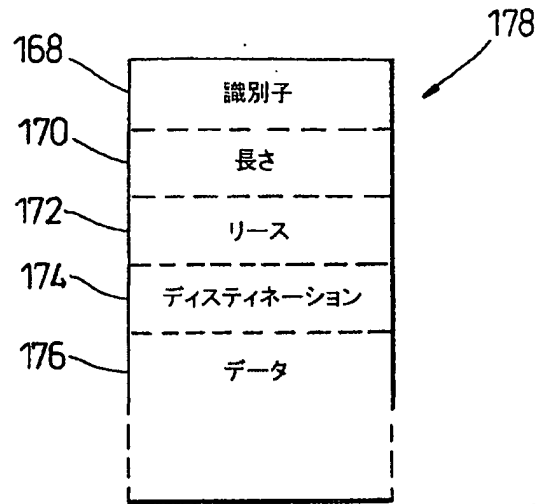
【図11】



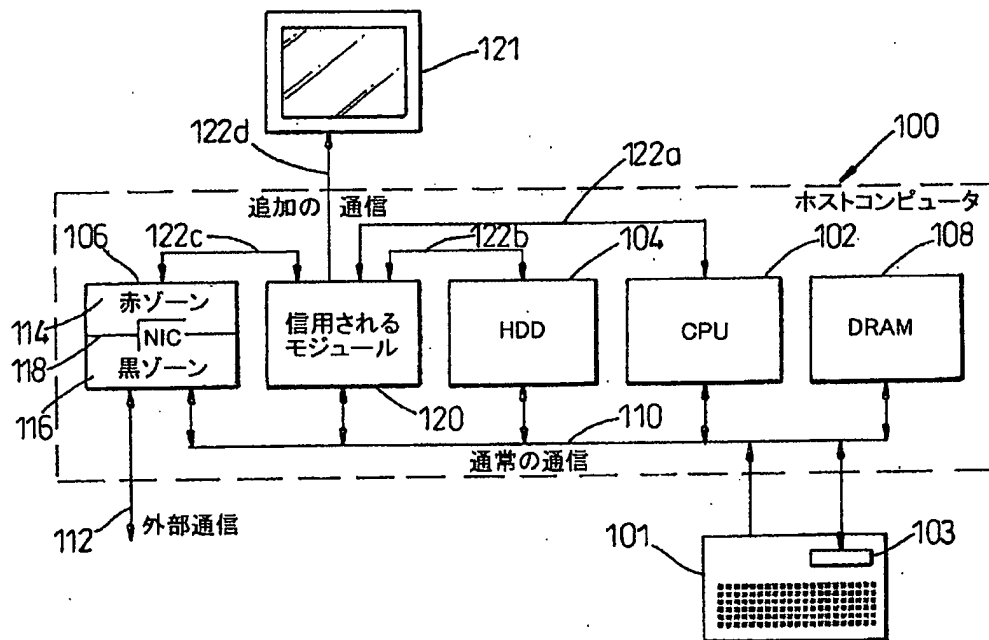
【図12】



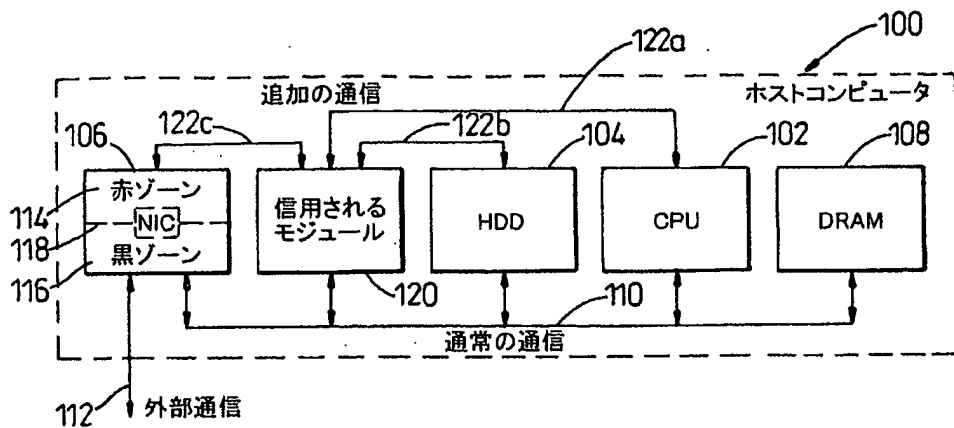
【図13】



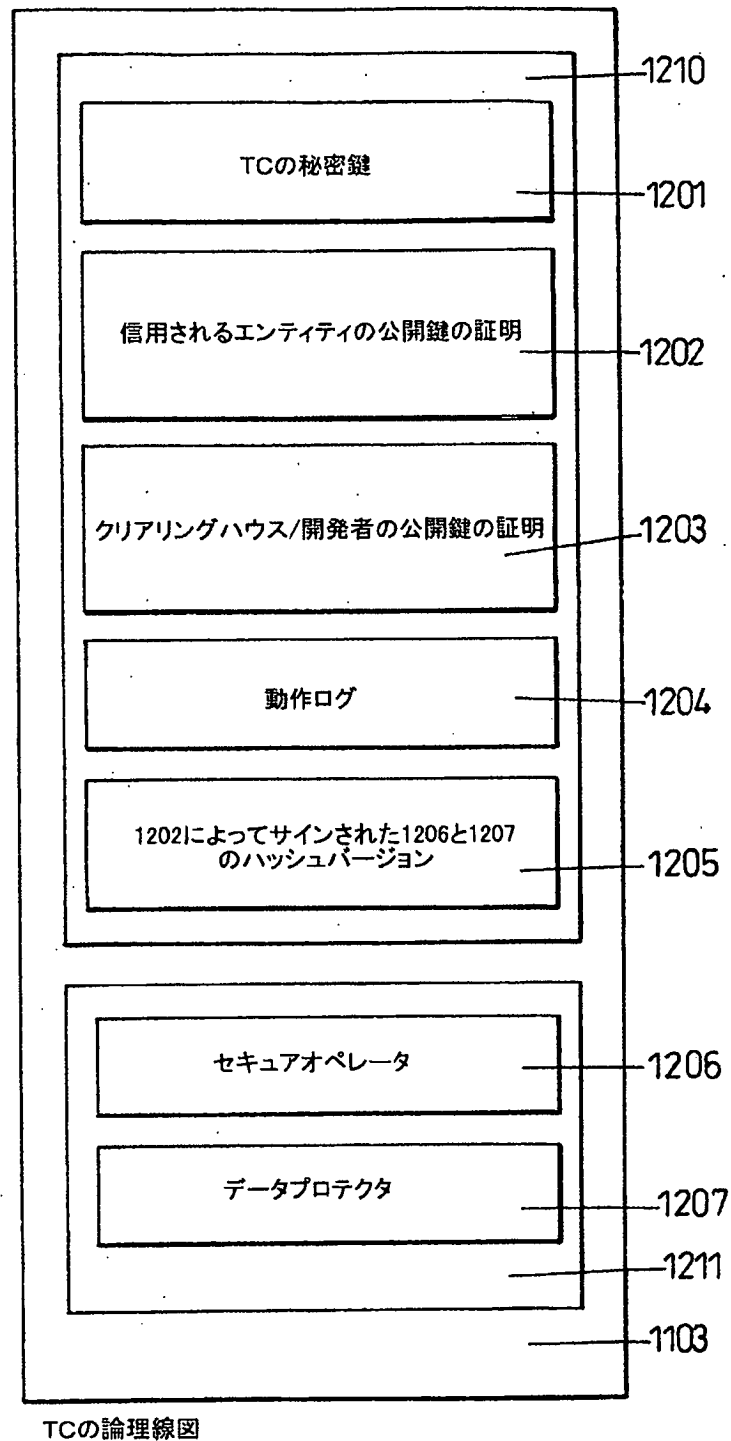
【図14】



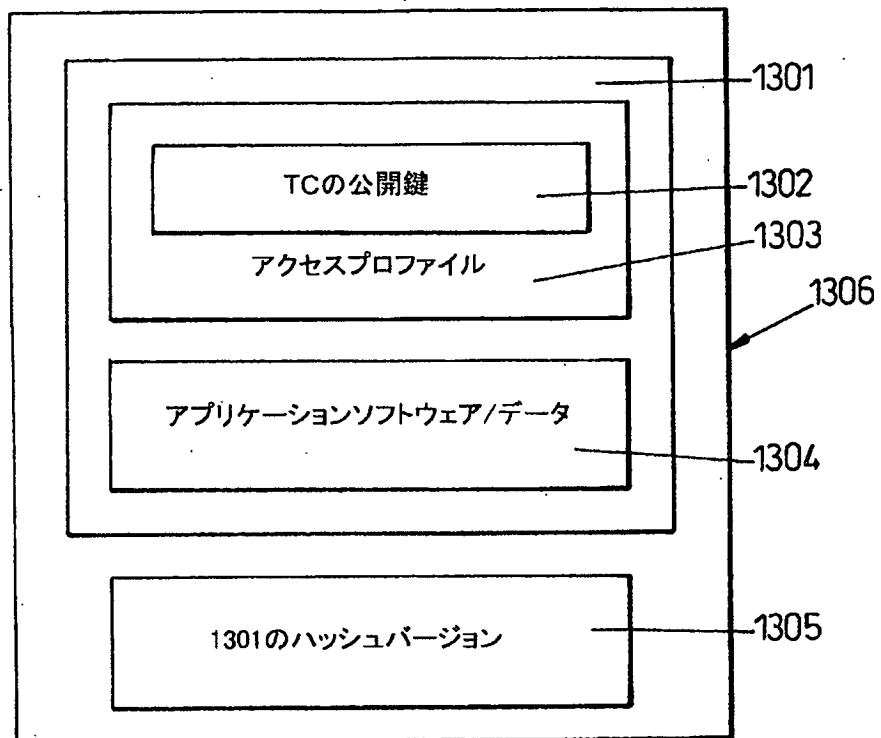
【図15】



【図16】

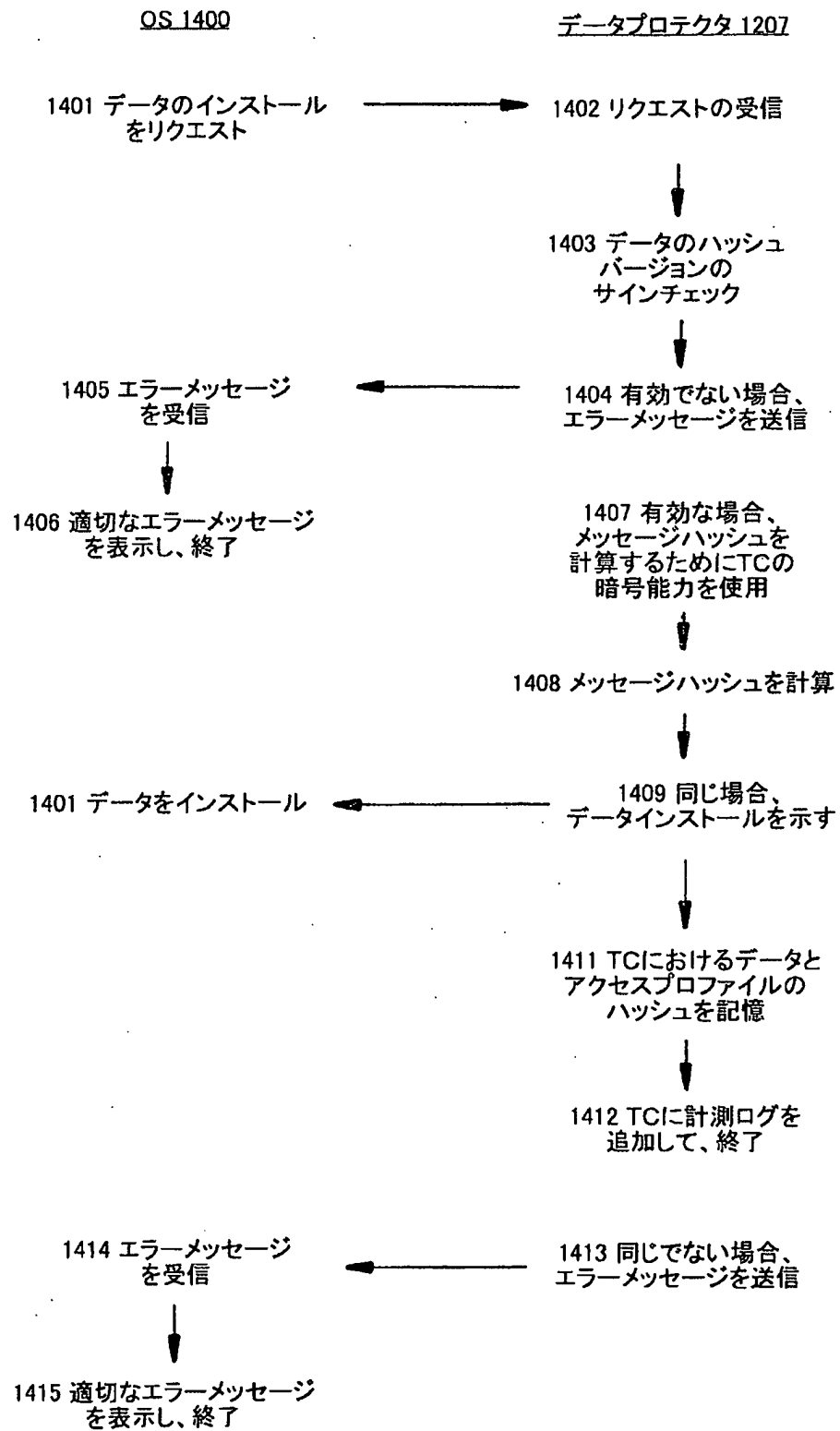


【図17】



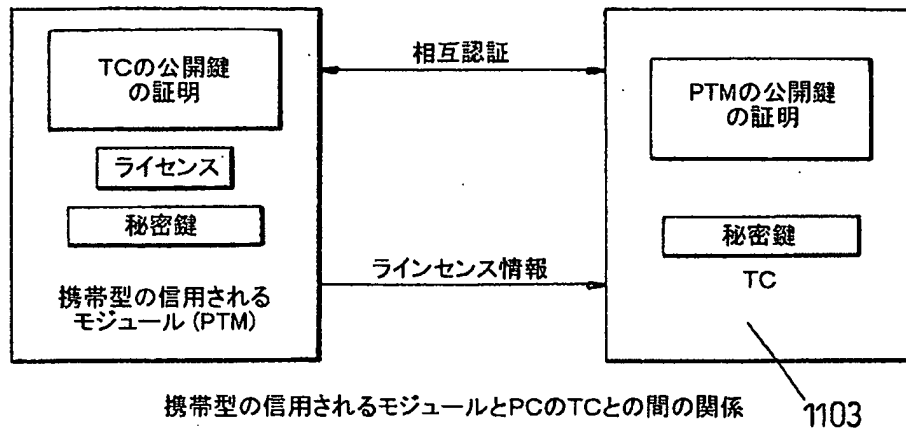
顧客のPCに搭載されたアプリケーション  
ソフトウェア/データの論理線図

【図18】

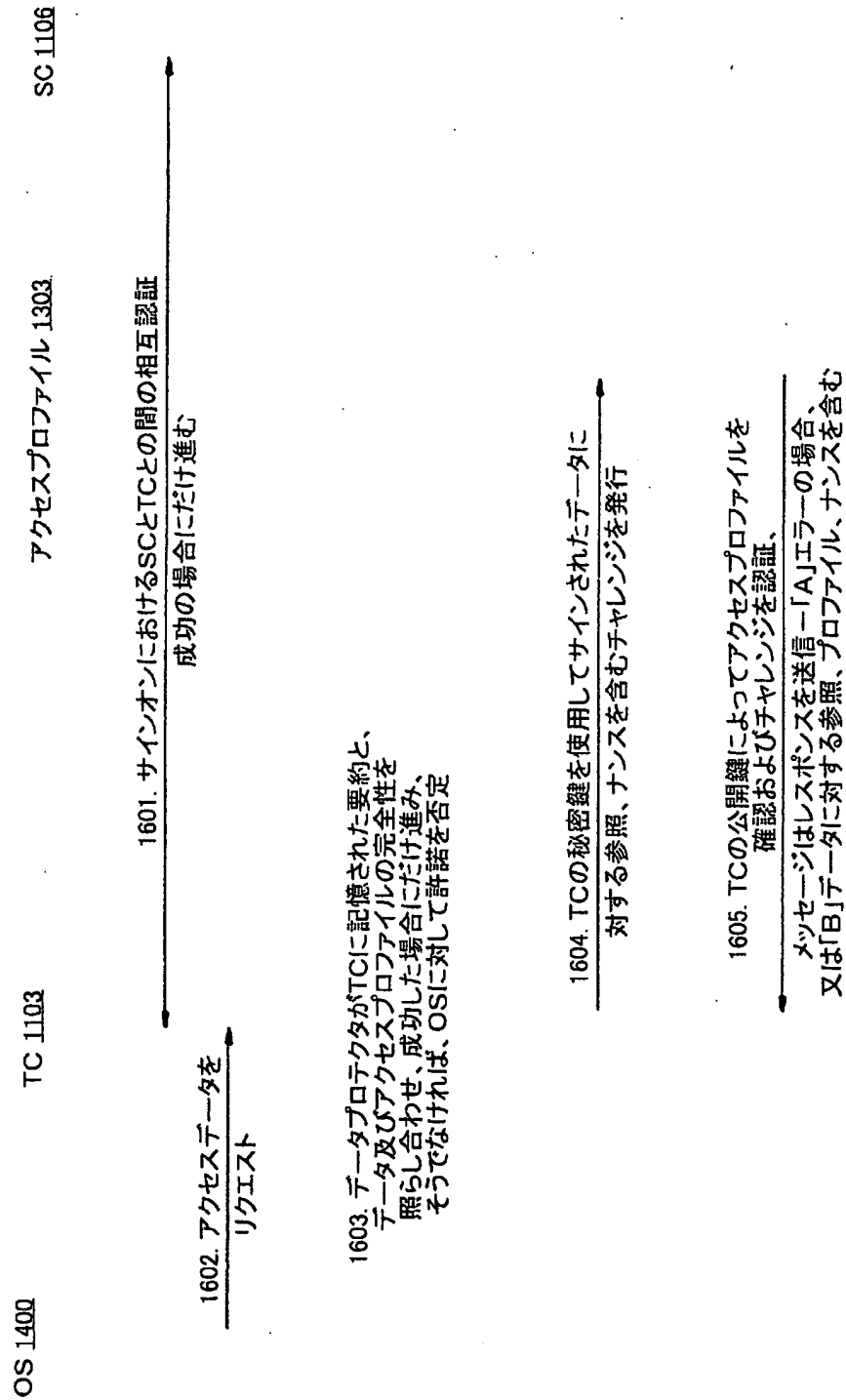




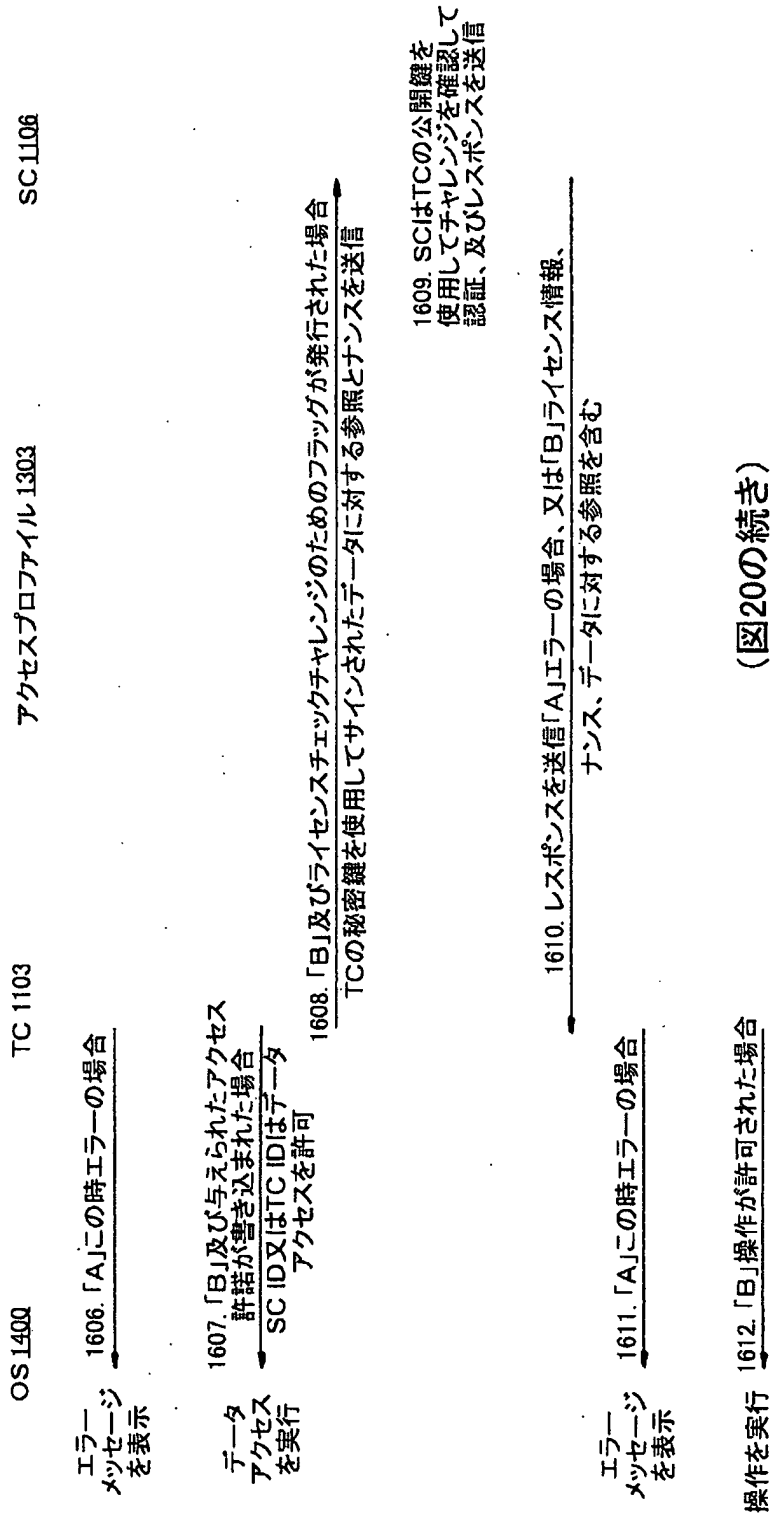
【図19】



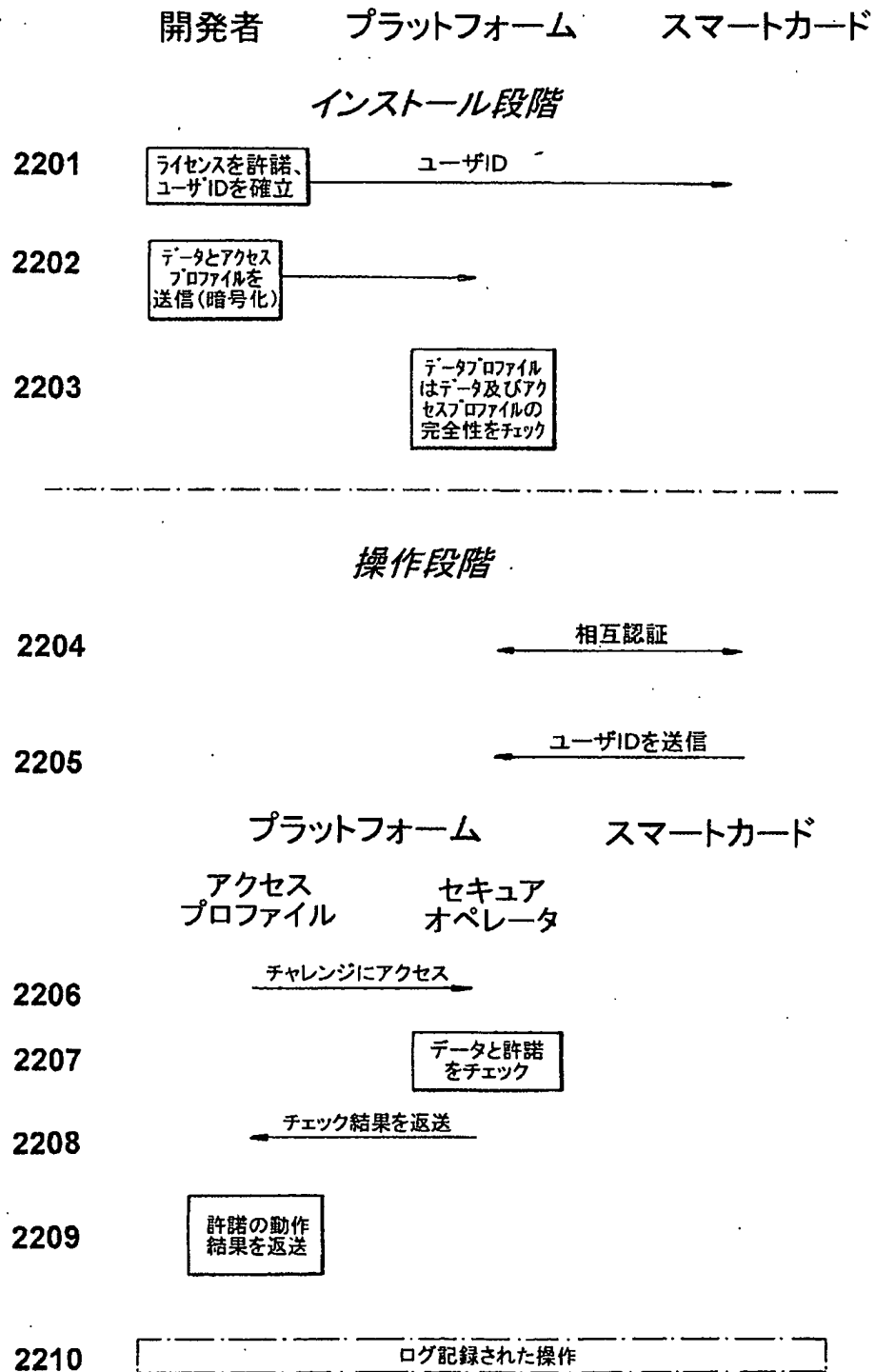
【図20のその1】



【図20のその2】



【図21】



## 【国際調査報告】

## INTERNATIONAL SEARCH REPORT

<b>A. CLASSIFICATION OF SUBJECT MATTER</b> IPC 7 606F1/00		<b>B. National Application No.</b> PCT/GB 00/03095
According to International Patent Classification (IPC) or to both national classification and IPC		
<b>B. FIELDS SEARCHED</b> Minimum documentation searched (classification system followed by classification symbols) IPC 7 606F		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used) EPO-Internal, WPI Data, PAJ		
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 933 498 A (ABRAMS MARSHALL D ET AL) 3 August 1999 (1999-08-03)  abstract; figures 3,14; table I column 7, line 1 - line 45 column 15, line 20 - column 17, line 12 column 21, line 10 - line 25 column 22, line 62 - column 25, line 5	1,4-8, 11,13, 18-20, 26,27, 30-32, 36,39-42
Y		2,3,9, 10,12, 14-17, 21,22, 24,25, 28,29, 33-35, 37,38
-/-		
<input checked="" type="checkbox"/> Further documents are listed in the continuation of box C.		
<input checked="" type="checkbox"/> Patent family members are listed in annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubt on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document relating to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "A" document member of the same patent family		
Date of the actual completion of the international search 22 January 2001		Date of mailing of the international search report 30/01/2001
Name and mailing address of the ISA European Patent Office, P.B. 5618 Patentplan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl Fax (+31-70) 340-3010		Authorized officer Powell, D

Form PCT/ISA/210 (second sheet) (July 1992)

page 1 of 2

## INTERNATIONAL SEARCH REPORT

International Application No.  
PCT/GB 00/03095

C. (Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	<p>-----</p> <p>SCHNECK P B: "PERSISTENT ACCESS CONTROL TO PREVENT PIRACY OF DIGITAL INFORMATION" PROCEEDINGS OF THE IEEE, IEEE, NEW YORK, US, vol. 87, no. 7, July 1999 (1999-07), pages 1239-1250, XP000955318 ISSN: 0018-9219 cited in the application page 1243, left-hand column, line 6 -page 1244, right-hand column, last line page 1246, right-hand column, line 13 - line 44 page 1249, left-hand column, line 12 - line 25</p> <p>-----</p>	1, 18, 27, 39, 40
Y	<p>US 5 473 692 A (DAVIS DEREK L) 5 December 1995 (1995-12-05)</p> <p>the whole document</p> <p>-----</p>	2, 3, 10, 12, 14-17, 21, 22, 24, 25, 28, 29, 33, 35, 37, 38
Y	<p>US 5 680 547 A (CHANG STEVE MING-JANG) 21 October 1997 (1997-10-21) the whole document</p>	9, 34
A		26
A	<p>-----</p> <p>EP 0 421 409 A (IBM) 10 April 1991 (1991-04-10)</p> <p>-----</p>	

## INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No.

PCT/GB 00/03095

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5933498 A	03-08-1999	AU 1690597 A	01-08-1997
		CA 2242596 A	17-07-1997
		EP 0880840 A	02-12-1998
		JP 2000503154 T	14-03-2000
		WO 9725798 A	17-07-1997
US 5473692 A	05-12-1995	AU 3583295 A	27-03-1996
		EP 0780039 A	25-06-1997
		JP 10507324 T	14-07-1998
		WO 9608092 A	14-03-1996
		US 5568552 A	22-10-1996
US 5680547 A	21-10-1997	US 5444850 A	22-08-1995
		AU 1042895 A	15-05-1996
		JP 10511783 T	10-11-1998
		WO 9613002 A	02-05-1996
EP 0421409 A	10-04-1991	US 5048085 A	10-09-1991
		CA 2026739 A,C	07-04-1991
		JP 3237551 A	23-10-1991
		US 5148481 A	15-09-1992

Form PCT/ISA/210 (patent family sheet) (July 1992)

---

フロントページの続き

(81)指定国 EP(AT, BE, CH, CY,  
DE, DK, ES, FI, FR, GB, GR, IE, I  
T, LU, MC, NL, PT, SE), JP, US

(72)発明者 プロウドラー, グレーム, ジョン  
イギリス国ブリストル・ビーエス34・8エ  
ックスキュー, ストーク・ギフォード, タ  
ッチストーン・アベニュー・5

Fターム(参考) 5B017 AA01 AA06 AA08 BA09 BB09  
CA15 CA16  
5B035 AA13 BB09 CA11 CA29  
5B076 AB10 AB17 FB01 FC10  
5B082 EA11